Algebra

（代数学）

模论及有限群常表示特征标理论

作者：代数表示论讨论班

时间：2023 年 4 月 20 日

序言

这是一份关于代数学中模论, 同调代数及有限群常表示论的讨论班讲义. 在全国大学生科研训练计划 (SRTP) 项目 « 模论及有限群常表示特征标理论 » 支持和项目导师李从辉老师的悉心指导下, 我们以模论和有限群表示论为主题开展了为期一年讨论班. 本讲义是在讨论班的基础上, 由西南交通大学数学学院 2020 级韦杰, 蔡羽珂, 李文科; 2019 级田玉亭; 2021 级胡佩诚, 2020 级物理学院张锦浩六位同学在李从辉老师的指导下完成的, 成书的本旨是为了对西南交通大学数学学院代数学方向高阶课程中相对基础的重要知识做一番介绍.

讲义以模论和有限群表示论为主线, 同时也广泛涉足了交换代数, 同调代数, 范畴论, 集合论, 代数表示论, 李理论及拓扑学等其它数学分支. 讲义主要参考的书籍是 Joseph.J.Rotman 的 Advanced Modern Algebra 上下两册. 本讲义是由讨论班讲稿整理而成, 但是限于我们自身知识结构尚不完整, 看待问题的角度更是无法高屋建瓴, 讲义中错误在所难免, 恳请各位老师、同袍、读者惠予指正.

讲义主要可以分成两个部分. 第一部分主要探讨模和模的范畴. 第一部分从基本模论出发, 介绍模和非交换环上的链条件研究模和环的有限性条件; 借助于 ZFC 公理体系, 介绍选择公理在代数学中的一系列等价命题; 引入范畴的语言, 介绍模的范畴, 并以此为出发点学习 Abel 范畴; 最后聚焦于 PID 上有限生成模的结构定理, 介绍基定理 (Basis Theorem) 和基本定理 (Fundenmental Theorem), 完成了有限生成 Abel 群的分类和线性代数中交换环上的矩阵环的分类.

讲义的第二部分主要探讨有限群的表示论, 其中以有限群的复表示为重点讨论了特征标理论. 第二部分从基本群论出发, 借助群作用这一工具学习了有限群的基本结构理论 (幂零群, 可解群, Sylow 定理等); 从模的观点, 同时借助同调代数的工具, 证明了有限群表示论的基本定理 Maschke 定理, 以及半单代数的重要结构定理 Artin—Wedderburn 定理和 Molien 定理. 在充分的结构理论基础上, 我们讨论了特征标, 类函数, 特征表标的正交关系; 并作为特征标理论的应用, 证明了 Burnside 定理和 Frobenius 定理. 至此, 讨论班画上圆满的句号.

一年以来, 讨论班在开展过程中遇到过许多困难. 最初大家不会使用 Latex, 也不习惯阅读英文书, 但经过一年以来的学习和交流, 我们在讨论班中不仅学到了优美的数学理论, 更是和彼此建立了深厚的情谊. 这一年中, 19 级学长田玉亭考研顺利上岸; 培养了 21 级学弟胡佩诚, 为代数方向留下了火种. 感谢大家一年来坚持参加讨论班, 感谢李从辉老师一年来无微不至的指导, 感谢刘品老师对讨论班的关心, 感谢西南交通大学数学学院对讨论班的支持. 愿大家未来无论在何种领域都能保持热爱, 都能发光出彩.

烟花易冷, 人事易分; 相逢有时, 后会无期. 我们谨以此书送给一路走来一起读书的朋友们, 同时也祝愿西南交通大学数学学院再创辉煌!

目录

第一章　模论

1.1　非交换环

到目前为止, 我们所研究的还都是交换环, 它的性质是很好的. 同样的, 我们可以把它的条件放宽一点, 把乘法运算中可交换的条件去掉, 发现关于环的定义它是合理的. 我讲的内容主要有非交换环的定义, 以群代数和除环作为例子, 再介绍子环的定义以及性质, 后面还有左理想右理想的概念, 以及环同态中像与核的概念, 其中群代数的构建与除环中四元数的概念将着重介绍.

定义 1.1.1. 环 R 是指有加法和乘法两种二元运算的集合, 其中 R 在加法下是 *Abel* 群, 任意 $a, b, c \in R$ 满足以下条件:

(1) $a(bc) = (ab)c$

(2) $a(b+c) = ab + ac; \quad (b+c)a = ba + ca$

(3) 存在$1 \in R$, 使得对于任意的$a \in R$: $1a = a = a1$.

注 1. 由上面的定义, 我们不难看出环 R 的交换性与所定义乘法的交换性有关.

下面是一些经典环结构的例子:

例 1.1.2. 如果 k 是任意交换环, 则 k 上的 n 阶方阵 $\mathrm{Mat}_n(k)$ 在矩阵加法和矩阵乘法下构成一个环. $\mathrm{Mat}_n(k)$ 是交换环当且仅当 $n = 1$. 如果环 k 不交换, 矩阵环 $\mathrm{Mat}_n(k)$ 也关于上述运算构成一个环. 这是因为通常矩阵乘法的定仍有意义: 如果 $A = (a_{ij})$ 和 $B = (b_{ij})$ 则乘积矩阵 AB 的第 i 行, 第 j 列元素是 $\sum\limits_{p} a_{ip}b_{pj}$, 这正好保证 A 中的元素恒出现在乘积左方, B 中的元素恒出现在乘积右方, 即环上的矩阵环之乘法运算不依赖于环的交换性.

例 1.1.3. k 是任意交换环, G 是一个阶为 n 的群, 我们定义群代数 kG: $|G| = n$, 其可表示为 $G = \{g_1, g_2, \cdots, g_n\}$. 任取域 F 上的一个 n 维向量空间 A. 取它的一组基. 由于在 G 中的元素两两不同. 我们取

$$g_1, g_2, \cdots, g_m$$

表示 m 个线性无关的向量, 再将其线性扩充到 n 个. 定义这组基元素的乘法为群的乘法. 由于线性扩充后对于两个元素之间的乘法与基元素是" 等价" 的, 则集合 $A(+,*)$ 中乘法 (群 G 的乘法) 满足结合律, 并且定义它与加法满足左右分配律. 于是, $(A,+,*)$ 就是一个环, 并且不难验证在关于数域 F 上还是一个代数, 称为群代数. 当然对于 $(A,+,*)$ 不一定是交换环.

例 1.1.4. 如果 $R_1,R_2,\cdots,R_t$ 是环, 则它们的直积 $R=R_1\times R_2\times\cdots\times R_t$ 关于坐标的点态加法和乘法构成一个环:

$$(r_i)+(r_i')=(r_i+r_i');\quad (r_i)(r_i')=(r_ir_i'),$$

其中, 我们把 $(r_1,r_2,\cdots,r_t)$ 简记为 (r_i). 特别地, 我们可以把 R_i 嵌入到直积 R 中, $r_i\in R_i$ 等同于第 i 个坐标是 r_i 而其他坐标都是零的" 向量". 如果 $i\neq j$, 则 $r_ir_j=0$.

例 1.1.5 (除环 D 或体). 称环 D 是一个除环, 若 $1\neq 0$, 并且对于任意的 $a\in D$ 都存在乘法逆: $a^{'}\in D$, 使得 $aa'=1=a'a$. 换句话说, 环 D 是除环当且仅当, 环 D 非零元素的集合 D^* 关于乘法构成群. 特别的, 域是除环.

下面是一个非交换环的例子。

例 1.1.6 (四元数代数). 设 $\mathbb{H}$ 是实数域 $\mathbb{R}$ 上四维向量空间, 标记其一个基为 $1,i,j,k$. 于是 $\mathbb{H}$ 中的一个典型元素 h 是:

$$h=a+bi+cj+dk;\quad a,b,c,d\in\mathbb{R}$$

我们定义基元素的乘法如下:

$$i^2=j^2=k^2=-1$$

$$ij=k=-ij;jk=i=-kj;ki=j=-ik$$

我们强调每个元素 $a\in\mathbb{R}$ 与 $1,i,j,k$ 可交换. 现在, 用线性扩张的方法定义 $\mathbb{H}$ 任意元素的乘法, 则 $\mathbb{H}$ 是环, 称为 (实) **四元数环** (乘法的结合性来自四元数群 $\{Q_8\}=\{\pm1,\pm i,\pm j,\pm k\}$ 中乘法的结合性). 事实上, 四元数环 $\mathbb{H}$ 是一个除环, 其中非零元素的逆如下. 定义 $u=a+bi+cj+dk\in\mathbb{H}$ 的共轭为:

$$\bar{u}=a-bi-cj-dk$$

易知,

$$u\,\bar{u}=a^2+b^2+c^2+d^2$$

因此, 当 $u\neq 0$ 时, $u\,\bar{u}\neq 0$, 从而:

$$u^{-1}=\frac{\bar{u}}{u\,\bar{u}}=\bar{u}(a^2+b^2+c^2+d^2)$$

不难证明共轭是加性同构并且满足:

$$\overline{uw} = \bar{w}\bar{u}$$

注 2. 关于四元数代数 $\mathbb{H}$, 我们有以下结论:
(1) $\mathbb{H}$ 是一个无限除环. 事实上, 有限除环必是域 (Wedderburn 定理)(2.5.1).
(2) $\mathbb{H}$ 是实数域 $\mathbb{R}$ 上的线性空间, 从而是一个 $\mathbb{R}-$ 代数.
(3) $\mathbb{H}$ 以 1 和 i, j, k 三者之一为基生成的子环同构于复数域 $\mathbb{C}$.
(4) $\mathbb{H}$ 中, 四元数群 Q_8 是非交换群, 但它的所有子群都是正规子群.
(5) $\mathbb{H}$ 中, 四元数群 Q_8 不同构于 8 阶二面体群 D_8. 原因在于, 他们有这不同的表示:

$$Q_8 = \langle x, y \mid x^2y^{-2}, y^4, xyx^{-1}y\rangle$$

$$D_8 = \langle x, y \mid x^2, y^4, xy^3xy\rangle$$

下面我们引入一个新的概念—子环. 环 R 的子环 S 是包含在 R 中的一个环, 满足 $1_R \in S$, 且对 $s, s' \in S$, 它们的和 $s + s'$ 和它们的积 ss' 在 S 中和在 R 中有相同的意义. 下面是正式定义.

定义 1.1.7. 环 R 的**子环** S 是指 R 的子集满足:
(1) $1 \in S$;
(2) 如果 $a, b \in S$, 则 $a - b \in S$;
(3) 如果 $a, b \in S$, 则 $ab \in S$.

根据子环的定义容易判断一个环的子集合是否为子环.

例 1.1.8. 下面分别给出子环和非子环的例子:
(1) 如果 D 是除环, 则它的中心 $Z(D)$ 是域. 此外, 如果 D^* 是 D 的非零元素的乘法群, 则 $Z(D^*) = Z(D)^*$, 即乘法群 D^* 的中心由 $Z(D)$ 的非零元素组成.
(2) 定义 $S = \{a + bi : a, b \in Z\} \subseteq \mathbb{C}$. 定义 S 中的加法, 而定义 S 中的乘法为:

$$(a + bi)(c + di) = ac + (ad + bc)i$$

于是在 S 中 $i^2 = 0$, 而在 $\mathbb{C}$ 中 $i^2 \neq 0$. 容易验证 S 是环, 但不是 $\mathbb{C}$ 的子环.

定义 1.1.9. 设 R 是环, 并设 I 是 R 的加法子群. 如果 $a \in I$ 和 $r \in R$ 蕴含 $ra \in R$ 则称 I 为左理想; 如果 $ar \in R$, 则称 I 为右理想. 如果 I 既是左理想又是右理想, 则称 I 为双边理想.

例 1.1.10. 在 $\mathrm{Mat}_2(R)$ 中. 等式

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} u & 0 \\ v & 0 \end{bmatrix} = \begin{bmatrix} * & 0 \\ * & 0 \end{bmatrix}$$

表明" 第一列"(即除第一行外都是 0 的矩阵) 形成一个左理想 (" 第二行" 也形成一个左理想).

$$\begin{bmatrix} u & v \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix}$$

表明" 第一行"(即除第一行外都是 0 的矩阵) 形成一个右理想.

当然可以验证这些单边理想没有一个是双边理想. 事实上, $\mathrm{Mat}_2(R)$ 双边理想只有

$$\{0\}, \mathrm{Mat}_2(R)$$

这个例子可以加以推广, 从而对每个环 k 和一切 $n \geq 2$ 给出 $\mathrm{Mat}_2(R)$ 中左理想和右理想的例子.

定义 1.1.11. 如果 R 和 S 是环, 则**环同态**是指函数 $\phi : R \longrightarrow S$, 对一切 $r, r' \in R$ 满足:
(1) $\phi(r + r') = \phi(r) + \phi(r')$.
(2) $\phi(rr') = \phi(r)\phi(r')$.
(3) $\phi(1) = 1$.
如果映射 $\phi : R \longrightarrow S$ 是环同态, 则**核**的定义和通常一样:

$$\mathrm{Ker}\,\phi = \{r \in R : \phi(r) = 0\}$$

像的定义和通常一样:

$$\mathrm{Im}\,\phi = \{s \in S : s \quad r \in R \;\; s = \phi(r)\}$$

注 3. 核 $\mathrm{Ker}\,\phi$ 恒为双边理想, 因为如果 $\phi(a) = 0$ 和 $r \in R$, 则:

$$\phi(ra) = \phi(r)\phi(a) = 0 = \phi(a)\phi(r) = \phi(ar)$$

从而,

$$a \in \mathrm{Ker}\,\phi \Rightarrow ra \in \mathrm{Ker}\,\phi, ar \in \mathrm{Ker}\,\phi$$

另一方面, $\mathrm{Im}\,\phi$ 只是 S 的子环.

1.2 环上的链条件

环和模上的链条件是研究环和模的有限性的工具. 得易于 Noether 引入链条件, 环论和模论中很多重要的证明得以简化. 链条件的有限性条件一般分为两种, Artin 条件和 Noether 条件. 根据 Hopkins—Levitzki 定理, 对于非交换环, Artin 的一定是 Noether 的; 但这样的性质对于模一般不成立. 特别地, 我们将证明 Hilbert 基定理. Hilbert 基定理指出了一大类有限生成多项式环. Hilbert 零点定理等工作是古典代数几何的基础.

我们首先回顾主理想整环上的链性质: R 是一个主理想整环, 则对于 R 的每条理想升链:

$$(a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \cdots \subsetneqq (a_n) \subsetneqq (a_{n+1}) \subsetneqq \cdots$$

都存在 $m \in N^+$ 使得:

$$(a_m) = (a_{m+1}) = (a_{m+2}) = \cdots$$

事实上, 这等价于 R 上的一个因子降链:

$$a_{i+1}|a_i, \text{存在} m \in N^+, \text{使得} n > m, \text{满足} a_{n+1} = a_n$$

特别地, 我们指出主理想整环的有限性保证了唯一因子分解的存在性. 一般的, 我们会问具有上述 "有限性条件" 的环是怎样的, 环上的 "有限性条件" 可以用什么可操作性的技术给出等价刻画? 下面我们回答这个问题.

定义 1.2.1. 若 R 是一个交换环, 称 R 是满足**升链条件** (Ascending Chain Condition, 简写为 ACC), 如果 R 的每条理想升链都有限。若 R 满足 ACC, 则称 R 是一个诺特环 (Noetherian ring).

定理 1.2.2 (诺特环的等价刻画). *R 是一个交换环, R 是一个诺特环, 当且仅当 R 的每一个理想都是有限生成的.*

证明. (必要性) 设 R 是一个诺特环. 若 I 是 R 的一个无限生成理想, 则存在序列:

$$a_1, a_2, a_3 \cdots$$

满足如下理想升链:

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

从而, 我们构造得到理想严格升链, 它不会停止.

(必要性) 任取 R 的理想升链:

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$$

令

$$I = \bigcup_{i=1}^{\infty} I_i$$

断言 $I = \bigcup\limits_{i=1}^{\infty} I_i$ 是一个理想. 而 I 是有限生成的, 所以存在

$$a_1, a_2, \cdots, a_n$$

使得

$$I = (a_1, a_2, a_3, \cdots, a_n)$$

从而

$$a_k \in I_{j_k}(k = 1, 2, 3, \cdots, n)$$

令

$$m = \max\{j_1, j_2, \cdots, j_n\}$$

$$I = (a_1, a_2, a_3, \cdots, a_n) \subset I_m \subset I$$

从而,

$$I = I_m$$

即得,

$$\forall n > m,\ I_n = I_m$$

故理想升链在有限步内停止. □

推论 1.2.3.
(1) PID 是诺特环.
(2) PID 是有限生成的, 因为它的每一个理想由一个元素生成.

现在, 我们同样可以把上述概念及结论放在非交换环当中讨论. 平行地, 我们以下仅以左诺特环为例子, 将相关概念及结论在非交换环当中进行推广.

定义 1.2.4. 称一个环 R 满足左理想升链条件 (ACC), 如果 R 的每条左理想升链

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots$$

会在有限步内停止.

同样地, 我们也可以定义右理想升链条件.

定义 1.2.5. R 是一个环 $U \subset R$, 则由 U 生成的左理想为所有有限的线性组合:

$$(U) = \left\{ \sum_{\text{finite}} r_i u_i : r_i \in R, u_i \in U \right\}$$

我们称左理想 I 是有限生成的, 若存在一个有限集 U 使得 $I = (U)$

注 4. 一些理想的生成元集有时也称为理想的一组基. 事实上, 生成元集是比线性空间的基 "弱" 的概念. 因为, 在一个理想的生成元集当中, 我们不能保证参数元素的线性表示唯一, 即表示 $c = \sum r_i u_i$ 不被参变量 c 唯一决定.

定义 1.2.6. 称一个环 R 是左 (右) 诺特环, 如果它的每一个左 (右) 理想都是有限生成的。

定理 1.2.7 (Noetherian 的等价刻画). *以下命题等价:*

(1) R *是一个左诺特环.*

(2) R *满足左升链条件 (Left ACC).*

(3) R *满足左极大条件:* R *的任何一个非空左理想集簇* $F \subset \{I \subset R | I$ *为* R *的左理想* $\}$*, 集簇* F *都存在极大元. (即存在* $M \in F$*, 使得不存在* $I \in F$*,* $M \subsetneqq I$*)*

(4) R *中的每一个左理想都是有限生成的.*

(5) 对于 R *中的每一个序列* $\{a_i\}_{i=1}^{\infty}$*, 存在* $m \geq 1$*, 使得* $r_1, r_2, \cdots, r_m \in R$*, 满足如下线性表示:*

$$a_{m+1} = r_1 a_1 + r_2 a_2 + \cdots + r_m a_m$$

证明. (1) $\Longleftrightarrow$ (2): 根据左诺特环的定义即知.

(2) $\Rightarrow$ (3): 令 $F \subset \{I \subset R | I$ 是 R 的左理想 $\}$, 我们假设 F 无极大元, 则取 $I_1 \in F$, I_1 不是极大元, 所以存在 $I_2 \in F$, 使得 $I_1 \subsetneqq I_2$; 同理, I_2 也没有极大元, 从而存在 $I_3 \in F$, 使得 $I_2 \subsetneqq I_3$. 以此类推, 我们可以得到理想升链

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$$

且不会停止, 与条件 (2) 矛盾.

(3) $\Rightarrow$ (4) : 考虑环 R 中所有有限生成的左理想构成的集簇 $G = \{I \subset R | I$ 是 R 中有限生成的左理想 $\}$. 首先注意到 $G \neq \phi$, 这是因为至少 $(0) \in G$. 下面证明: $G = \{I \subset R | I$ 是 R 的左理想 $\}$. 任取 R 中的理想 I, 欲证 I 是有限生成的. 考虑集合 $G = \{N \subset I | N$ 是 R 中有限生成的理想 $\}$, 则根据 (3) 知, 存在极大元 $M \in G$, 使得 $M \subset I$. 断言: $M = I$, 否则, $\exists a \in I$, $a \notin M$, 则集合 $J = \{m + ra | m \in M, r \in R\} \subset I$ 是一个左理想 (容易验证), 而这与 M 的极大性矛盾. 故 I 是有限生成的.

(4) $\Rightarrow$ (2) : 考察环 R 中的任意一条理想升链: $I_1 \subset I_2 \subset \cdots I_n$. 令 $I = \bigcup\limits_{i=1}^{\infty} I_i$, I 为一个左理想. 根据 (4), I 是有限生成的, 类似与诺特环的等价刻画定理的证明, $\exists a_1, a_2, \cdots, a_q \in R$, 使得 $I = (a_1, a_2, \cdots, a_q)$, 存在 N, $I = (a_1, a_2, \cdots, a_q) \subset I_N \subset I$.

(1) $\Rightarrow$ (5) : 设 $\{a_1, a_2, \cdots, a_n, \cdots\}$ 为 R 中的一个序列. 令 $I_1 = (a_1), I_2 = (a_1, a_2), \cdots, I_n = (a_1, a_2, \cdots, a_n)$, 根据左理想升链条件:$\exists m \geq 1$, 使得 $I_m = I_{m+1}$, 所以 $a_{m+1} \in I_{m+1} = I_m$, 从而 $\exists r_i \in R$, $a_{m+1} = \sum\limits_{i=1}^{m} r_i a_i$, 即证.

(5) $\Rightarrow$ (1) : (反证法): 假设 R 满足序列条件, 但 R 不是诺特环, 则存在一条左理想升链:

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$$

不会停止. 对于 $\forall n \in N$, 选取 $a_{n+1} \in I_{m+1}, a_{n+1} \notin I_n$, 这与序列条件矛盾. □

定理 1.2.8 (Hilbert Basis Theorem). R *是左诺特环, 则* $R[x]$ *也是诺特环.*

证明. (Sarges) (反证法): 假设 I 是 $R[x]$ 上的左理想, 且理想 I 不是有限生成的, 则 $I \neq (0)$. 定义: $f_0(x)$ 为 I 上次数最小的多项式 (自然数集有下确界可以保证). 归纳地, 我们可以定义 $f_{n+1}(x)$ 为 $I^* = I - (f_0, f_1, \cdots, f_n)$ 上次数最小的多项式. 注意, $\forall n > 0$, $f_n(x)$ 是存在的, 因为 I 不是有限生成的, 故 $I - (f_0, f_1, \cdots, f_{n-1}) \neq \phi$. 于是, 我们得到

$$deg(f_0(x)) \leq deg(f_1(x)) \leq \cdots \leq deg(f_n(x)) \leq \cdots$$

记 $a_n \in R$ 为 $f_n(x)$ 的首项系数, 根据诺特环的等价刻画, $\exists m \in N$,$\exists r_i \in R(i = 1, 2, 3, \cdots, m)$ 使得 $a_{m+1} = \sum_{i=1}^{m} r_i a_i$.

定义:

$$f^*(x) = f_{m+1}(x) - \sum_{i=1}^{m} x^{d_{m+1}-d_i} r_i f_i(x)$$

其中, $d_i = deg(f_i(x))$.

注意到 $deg(f^*(x)) = m$, 这是因为 $deg(\sum_{i=1}^{m} x^{d_{m+1}-d_i} r_i f_i(x)) = d_{m+1} = deg(f_{m+1}(x))$, 而 $a_{m+1} = \sum_{i=1}^{m} r_i a_i$. 因此, $f^*(x) \in I - (f_0, f_1, \cdots, f_m)$; 同时, 根据 f^* 和 f^{m+1} 的构造知, $f^*(x) \in I - (f_0, f_1, \cdots, f_{m+1})$, 且 $deg(f^*(x)) < deg(f_{m+1}(x))$, 这与 $f_{m+1}(x)$ 的选取矛盾, 即 $R[x]$ 为诺特环. □

推论 1.2.9.

(1) 若 R 是诺特环, 则 $R[x_1, x_2, \cdots, x_n]$ 是诺特环.

(2) k 是一个域, $k[x_1, x_2, \cdots, x_n]$ 是诺特环.

(3) Z 是 *PID*, 则 $Z[x_1, x_2, \cdots, x_n]$ 是诺特环.

(4) 对于 $k[x_1, x_2, \cdots, x_n]$ 中任何一个理想 I, 其中 k 是域或者是 *PID*, 则商环

$$k[x_1, x_2, \cdots, x_n]/I$$

是诺特环.

下面, 我们列出关于诺特环的一些性质, 它们的证明是容易的.

性质 1.2.10.

(1) R 是左诺特环, I 是 R 的双边理想, 则商环 R/I 也是左诺特环.

(2) 每一个左诺特环中, 都有极大左理想.

(3) k 是一个域, 则 k 上的有限维代数 A 即是 *Artin* 的, 又是 *Noether* 的. 注释: 我们称一个环 A 是 k——代数 (k 是环 A 的一个子环), 如果定义在 k 上的数乘可以与任何事物交换.

$$(\alpha u)v = \alpha(uv) = u(\alpha v); \alpha \in k; u, v \in A$$

对偶地, 我们对于满足左理想降链, 也可以有上述类似讨论.

定义 1.2.11. 称环 R 的理想链为左理想降链 (DCC), 若环 R 的左理想满足关系:

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq \cdots$$

且会在有限步内停止.

定义 1.2.12. 如果一个环 R 满足上述的左理想降链 (DCC) 条件, 则称它是一个 Artin 环.

定理 1.2.13 (Artin 环的等价刻画). *以下命题等价:*

(1) 环 R 是一个 Artin 环.

(2) 环 R 满足左理想降链条件 (DCC).

(3) 环 R 满足左极小条件: 对于任意的 $F \subset \{I \subset R | I$ 是 R 的左理想$\}$, 存在 $M \in F$, 使得不存在 $B \in F$, 有 $B \subsetneqq M$ 成立.

注 5. 值得说明的是:

(1) 一个环不需要包含极小 (左) 理想, 但一定包含极大 (左) 理想 (用 Zorn 引理可证). 例如, 整数环 Z 没有极小理想: $I = (n) \supsetneqq (2n) \supsetneqq \cdots \supsetneqq (2^k n) \neq (0); \forall k \in N$。

(2) 整数环 $\mathbb{Z}$ 是左诺特环, 但不是左阿廷环.

$$\mathbb{Z} \supsetneqq (2) \supsetneqq (2^2) \supsetneqq (2^3) \supsetneqq \cdots$$

不会停止.

(3) 若环 R 是 Artin 的, 则一定是 Noether 的 (阿廷环是比诺特环更强的概念).

1.3 左模与右模

我们学习过群, 环, 域, 线性空间和结合代数等代数结构, 下面我们将介绍一种新的代数结构—模. 模可以作为线性空间的推广, 也可以看作是环对 Abel 群的作用 (表示) 所得到的一个新的结构. 我们会给出一些经典的例子, 并以之为切入点介绍两种构造模的方法. 最后, 类似于群和环, 我们介绍对于模的同构基本定理及对应定理.

定义 1.3.1. 设 R 是个有单位元的环, M 是个 Abel 群. 现建立 R 上的左 $R-$ 模 M 是一种有类似向量的标量计算系统, 准确来说也就是对于任意的 $r \in R$, $m \in M$ 有二元映射:

$$R \times M \to M$$

$$(r, m) \to r.m$$

满足如下法则:

(1) $r.(m+m^{'})=r.m+r.m^{'}$

(2) $(r+r^{'}).m=r.m+r^{'}.m$

(3) $(rr^{'}).m=r.(r^{'}m)$.

(4) $1.m=m$

定义 1.3.2. 建立在 R 上的右 $R-$ 模也是类似的, 对于任意的 $r\in R$, $m\in M$ 有二元映射::

$$M\times R\to M$$

$$(m,r)\to mr$$

满足:

(1) $(m+m^{'}).r=m.r+m.^{'}$.

(2) $(r+r^{'}).m=r.m+r^{'}.m$.

(3) $m.(rr^{'})=(m.r.)r^{'}$

(4)$^{'}m.1=m$.

此时建立在 R 上的左 R 模 M 可以记作 ${}_RM$, 相应的右 R 模记作 M_R.

其实, 我们已经见过了很多模的例子. 现在只是把这些运算规则做进一步的提炼推广, 比如考虑 $R[X]$ 上的多项式; 其求导算子 D 自然构成自身到自身的线性映射, 且时常有诸如这样的简便记法

$$(1+D)^2f=(D^2+2D+1)f$$

此时我们已经有了一种把算子, 也就是线性空间 $R[X]$ 上的变换全体 $\mathrm{End}(R[X])$(自然, 这可以构成一种环, 其单位 1_R 是恒等映射) 作为一种左乘的“标量”来看待.

注 6. 在左 (右) 模中, 需要注意的地方是, 左与右理论上地位是相等的. 如果你是阿拉伯人, 那么对你而言左模的 (1), (2), (4) 性质就是一般地球人眼中右模的性质; 但对于条件 (3), 左与右有本质差异. 在左模中, 先与 m 结合的是 r'; 而在右模中, 则是 r. 这个事实不会因你的阅读顺序改变而不同. 自然, 如果是环 R 是可交换的, 那么以上 4 条关于左模和右模的定义将无任何区别. **出于对称的美学来看, 建立在左右模上的定理应当是相似的或是对偶的. 下面出于习惯, 我们主要考虑左模, 对于右模定理的相同性不再赘述**.

以下是更多左模的例子:

例 1.3.3. 事实上, 任意建立在数域 k 上的线性空间本身就是个 $k-$ 模.

例 1.3.4. 对于数域 k 上的向量空间 V, 若给出线性变换 $A:V\to V$, 且对任意的 $v\in V$ 及任意多项式 $f(x)\in k[x]$, 定义运算:

$$f(x).v=f(A)(v)=a_0v+a_1Av+\cdots+a_kA^kv$$

从而我们赋予了 $k[x]-$ 左模的结构. 取 A 为开头的求导算子 D, 则得到了最初的例子. 特别的, 对于线性变化, 在线性空间取定一组基的情况下, 我们可以使用坐标相应的矩阵来具体的刻画变换本身, 此时不难想到会有矩阵环 $\mathrm{Mat}_n(k)$ 作用于 k^n 的 n 维向量构成 $\mathrm{Mat}_n(k)-$ 模.

例 1.3.5. 对于一个环 K, 其任意的左理想 J 自然构成一种 $K-$ 模. 此时二元运算的定义即为环的普通乘法:

$$x.y = xy \in J, x \in K, y \in J$$

特别的, 当取 $J = K$ 时, 此时也就是环 K 自身关于自身构成模。

定义 1.3.6. 若建立在相同的含单位 1_R 的环 R 上的两个模 M, N 如果满足下列式子, 则称 $\phi : M \to N$ 为 $R-$ **模同态**: 对于任意的 $r \in R, m, m^{'} \in M$ 我们有:

(1) $f(m + m^{'}) = f(m) + f(m^{'})$.

(2) $f(r.m) = r.f(m)$.(对于右模就是 $f(m.r) = f(m).r$) 特别留意的是两个 Abel 群 M, N 要求其标量运算建立在相同的含幺环 R 上.

进一步的, 如果 f 为双射, 则称 f 为**模同构 (isomorphism)**.

定义 1.3.7. 模同态 $f : M \to N$ 的**核 (kernel)** 为:

$$\mathrm{Ker}(f) = \{m \in M \mid f(m) = 0_N\}$$

像 (image) 为:

$$\mathrm{Im}(f) = f(M)$$

定义 1.3.8. 一个**环** R 的表示 (**Representation**) 是指环同态:

$$\sigma : R \to \mathrm{End}_R(M)$$

其中 M 是一个 Abel 群, $\mathrm{End}_R(M)$ 是 $R-$ 模 M 的模自同态环. 特别地, 若是 σ 为同构, 则称其为**忠实的** (faithful).

我们把群的线性表示的定义列出以显示他们之间具有的联系.

定义 1.3.9 (群 G 的线性表示). 设 G 是个群, V/k 是域 k 上的线性空间, 称群同态

$$\Phi : G \to \mathrm{GL}(V)$$

为群 G 关于线性空间 V 的一个域 k 上的**线性表示 (linear representation)**. 其中, $\dim_k(V) = n$, $\mathrm{GL}(V)$ 是 V 上全体可逆线性变换构成的集合 (即 V 的自同构群, 区别于 $\mathrm{End}(V)$ 自同态环). 特别地, 如果 $\mathrm{Ker}\,\Phi = e_G$, 则称这个线性表示为**忠实的 (faithful)**. n 称为**表示的维数 (dimension of representation)**. 线性表示实质上就是由表示空

间 V 和群同态 $\Phi : G \to \mathrm{GL}(V)$ 构成的二元组, 一般记为 (Φ,V). 注意到, $\mathrm{GL}(V)$ 在线性空间 V 取定一组基 $e_1, e_2, \cdots, e_n$ 的情况下同构于一般线性群 $\mathrm{GL}(n, k)$. 从而, 我们得到更有价值的群同态映射:

$$\psi : G \mapsto \mathrm{GL}(n, k)$$

ψ 通过矩阵来刻画群的结构, 实现从抽象到具体的过渡. ψ 称为**矩阵表示 (matrix representation)**.

一开始我们定义模时, 二元映射:

$$R \times M \to M$$

可以理解为把环 R 中的元素视作某种作用到 Abel 群 M 上的算符, 而正如一开始的例子中的求导算子那样. 这样可以通过研究 $\mathrm{End}_R(M)$ 来反应 R 的性质 (本质上即为环的表示). 关于这点, 我们可以严谨的阐述一下:

性质 1.3.10. *每一个环表示 $\sigma : R \to End(M)$ 可以唯一决定一种建立在 Abel 群 M 上的左 $R-$ 模; 反过来, 一种 M 上的左 R-模也将唯一对应一种环表示 $\sigma : R \to \mathrm{End}(M)$.*

证明. 对给定的一个环表示 $\sigma : R \to \mathrm{End}(M)$, 记 $\sigma(r) \in \mathrm{End}(M)$ 为 σ_r. 现在 σ 诱导了一种 $R \times M \to M$ 的映射, 由此自然定义了一种 M 上的标量运算为:

$$r.m = \sigma_r(m)$$

可以验算这的确满足左模标量运算的四条定义. 其中 σ_{1_R} 自然是恒等映射, 这是由环同态 σ 的同态性质决定的.

反过来, 对于具有建立在环 R 上标量运算结构的 Abel 群 M, 可以由标量运算 $r.m$ 定义映射:

$$T_r : M \longmapsto M$$

$$m \longmapsto r.m$$

容易验证上述映射 $T : R \to \mathrm{End}(M)$ 是环同态, 即也是 R 的表示. □

注 7. 环的表示并不唯一, 唯一的是当表示确定时, 可以相应唯一确定一个左模.

定义 1.3.11. 设 V 是左 $R-$ 模, $U \subset V$ 是 V 的子群, 若对于任意的 $x \in R, u \in U$, 我们有 $x.u \in U$(即 U 上关于 R 的标量运算封闭), 则称子群 U 称为 V 的**左子模 (left submodule)**.

例 1.3.12. 下面我们给出一些子模的例子:
(1) R-模 V 上的任意多个子模 $V_i \subset V$ 的交 $\bigcap\limits_i V_i \subset V$ 仍然为一个子模.

(2) 设 R 为一个环, 则 R 关于自身构成正则 $R-$ 模. 此时对于 $T \subset R$, T 是左 $R-$ 子模, 当且仅当 T 是环 R 的左理想.

(3) 对于一个 $R-$ 模 M, 比较重要的一个子模是模同态 f 的核 $\mathrm{Ker}(f)$. $\mathrm{Ker}(f)$ 作为加群的子群是显然的, 其次对于任意的 $x \in R, m \in \mathrm{Ker}(f), f(x.m) = x.f(m) = 0$, 于是 $x.m \in \mathrm{Ker}(f)$. 由此, 我们可以构造商模 $M/\mathrm{Ker}(f)$.

定义 1.3.13. R 是一个环, U 是 $R-$ 模 V 的子模. 如果环 R 上的子模 $U \subseteq V$ 对任意 $x \in R$ 满足商群 V/U 的加法和如下定义的数乘:

$$V/U = \{v + U \mid v \in V\}$$

$$x.(v + U) = x.v + U$$

则容易验证 V/U 也是个 R-模, 称为 V 关于子模 V 的**商模 (quotient submodule)**.

定理 1.3.14 (模的第一同构定理). *设 M, N 为 $R-$ 模, $f : M \to N$ 是 $R-$ 模同态. 则 $\mathrm{Ker}(f)$ 是 M 的子模, 且如下模同构 ϕ 成立:*

$$\varphi : M/\mathrm{Ker}\, f \to \mathrm{Im}(f)$$
$$m + \mathrm{Ker}\, f \mapsto f(m)$$

证明. 模同态的首先是 Abel 群 M, N 的同态, 这从群的第一同构定理可以推出. 其次, 我们需要验证模同态保持标量乘法:

$$\begin{aligned}\varphi(r.(m + \mathrm{Ker}(f))) &= \varphi(r.m + \mathrm{Ker}(f)) \\ &= f(r.m) \\ &= r.f(m) \\ &= r.\varphi(m + \mathrm{Ker}(f))\end{aligned}$$

其中, $\mathrm{Ker}(\varphi) = \mathrm{Ker}(f)$. □

定理 1.3.15 (模的第二同构定理). *设 S, T 为左 $R-$ 模 M 的子模, 则如下模同构成立:*

$$S/(S \cap T) \cong (S + T)/T$$

证明. 考虑自然同态

$$\pi : M \to M/T$$
$$m \to m + T$$

其中, $\mathrm{Ker}\, \pi = T$, 将 π 限制到子模 S 上, 记限制映射为:

$$\pi\,|_S \colon s \mapsto \pi(s)$$

此时限制态射的核和像为:

$$\operatorname{Ker}\pi\mid_S = T\cap S$$

$$\operatorname{Im}\pi\mid_S = \{s+T\mid s\in S\} = S+T$$

再由第一同构定理(1.3.14)可知 $S/(S\cap T)\cong S+T/T$. □

定理 1.3.16 (对应定理 (Correspondence Theorem)). *设 T 是左 $R-$ 模 M 的一个子模, 记其商模 M/T 为 $\overline{M}$. 则存在如下的双射 φ:*

$$\{S\leqslant M\mid T\subset S\subset M\}\longleftrightarrow\{\overline{S}\leqslant\overline{M}\mid\overline{S}\subset\overline{M}\}$$

其中,

$$\varphi: S\mapsto\overline{S}$$

此外, ϕ 保持序关系, 也就是说

$$S\subset S^{'}\Leftrightarrow\overline{S}\subset\overline{S'}$$

证明. 注意到到命题中涉及的集合 T,S,M 实质上都是交换的加群及其子群. 由群的对应定理, 可以之间说明上述双射 φ 的存在性. 唯一值得提及的就是 S 的对应 $\overline{S}$ 是具有模的结构. 而这也是显然的, 因为 S/T 自然可构成商模. □

注 8. 注意到 φ 不构成同态, 事实上上述两个集合连运算结构都没有赋予.

定理 1.3.17 (第三同构定理). *设 M 为一左 R-模, 其子模 T,S 满足 $T\subset S\subset M$, 按对应定理, 分别有对应 $\overline{M}=M/T;\overline{S}=S/T$; 则如下同构*

$$M/S\cong\overline{M}/\overline{S}=(M/T)/(S/T)$$

证明. 考虑自然同态 $\sigma: M\to\overline{M}=M/T$, 与自然同态 $g:\overline{M}\to\overline{M}/\overline{S}$.
同态的复合还是同态, 于是得到 $M\to\overline{M}/\overline{S}$ 的同态 $g\sigma: m\mapsto\overline{m}+\overline{S}$. 计算其同态核

$$\begin{aligned}\operatorname{Ker} g\sigma &= \{m\in M\mid g\sigma(m)=\overline{0}+\overline{S}\} &(1.1)\\ &= \{g(\overline{m})=\overline{0}+\overline{S}\} &(1.2)\\ &= \{\overline{m}\in\overline{S}\} &(1.3)\\ &= S &(1.4)\end{aligned}$$

根据模第一同构定理可得 $M/S\cong\overline{M}/\overline{S}$. □

定义 1.3.18. 设 V 是一左 $R-$ 模, 取 V 上一集合 T, 记

$$\langle T\rangle = \left\{ \bigcap_{r\in\Gamma} V_\gamma \;\middle|\; T\subset V_\gamma \subset V,\ V_\gamma \text{ 是子模} \right\}$$

即 $\langle T\rangle$ 是全体包含集合 T 的子模 V_γ 的交, 它是个新的子模. 此时称这个子模是**由集合 T 生成的 (generated by T)**, 生成集合为 T.

性质 1.3.19. *R 是一个环, M 是一个 $R-$ 模, $T\subseteq M$ 是一个集合, 以下性质为 $\angle T\rangle$ 的等价刻画:*

(1) 集合 T 生成的子模 $\langle T\rangle$ 是包含 T 的最小的子模.

(2) $\langle T\rangle$ 中元素可被具体写成如下有限和形式:

$$r_1t_1 + r_2t_2 + \cdots + r_st_s; \text{其中} r_i\in R, t_i\in T$$

证明. (1) 由 T 生成的定义容易得 $\langle T\rangle$ 为最小包含 T 的子模. 否则若有更小包含 T 的子模 $W\subseteq\langle T\rangle$. 显然 $W\in\{V_\gamma \mid \gamma\in\Gamma, \text{子模} V_\gamma\supset T\}$, 那么有 $\langle T\rangle\subset W$, 此时有 $W=\langle T\rangle$.

(2) 记 $K=\{\sum r_it_i \mid r_i\in R, t_i\in T\}$. 根据子模对数乘封闭而得 $K\subset\langle T\rangle$. 取 $r_i=1, i=1$, 显然可知 $T\subset K$. 由上条 $\langle T\rangle$ 为最小含 T 子模性质可知 $\langle T\rangle\subset K$. 由此 $K=\langle T\rangle$ 得证.

□

注 9. 根据上述性质, 我们有如下特例:

(1) 当一个模 M 可由一有限集生成, 则称 M 是**有限生成的 (finitely generated)**. 对于一般的有限维的向量空间, 他们自然都是有限生成的.

(2) 当生成集 $T=\{x\}$ 为单点集时, $\langle T\rangle = Rx$ 称为**循环模 (cyclic module)**.

(3) S,T 为 M 的两个子模, 我们有 $S+T=\langle S\cup T\rangle$. 首先 $S+T$ 是包含 $S\cup T$ 的子模, 由性质 (1) 知 $\langle S\cup T\rangle\subseteq S+T$; 另一个方向考虑 $S+T$ 中任意元素 $1s+1t\in\langle S\cup T\rangle$(性质 (2)) 可得.

定义 1.3.20. R 是一个环, M 是一个 $R-$ 模. 对任意的 $r\in R, 0\neq m\in M$ 可构造如下态射:

$$\sigma : R \longmapsto M$$

$$r \longmapsto rm$$

容易验证 σ 构成 ${}_RR$ 到 ${}_RRm$ 的模同态, 其中 Rm 是由单元素 m 生成的循环模. 映射的核 $\mathrm{Ker}(\sigma)$ 可特别地记作:

$$\mathrm{ann}_R(m)=\{r\in R \mid r.m=0\}$$

称其为元素 m 的**零化子 (annihilator)**. 特别地, 第一同构定理给出了同构:

$$R/\operatorname{ann}(m) \cong Rm$$

其中, 若 m 对应的零化子 $\operatorname{ann}(m) \neq \{0\}$, 则存在非零标量 $r \in R$ 使得 $rv = 0$. 此时, 称 v 是**有挠的 (torsion)**. 若所有模中元素都是有挠的, 则称这个模是**挠模 (torsion)**; 若模 M 中没有非零挠元, 则称这个模是**无挠模 (torsion—free)**.

定义 1.3.21. R 是一个环, M 是一个 $R-$ 模. 记:

$$\operatorname{ann}(M) = \{r \in R \mid rM = 0\} = \bigcap_{m \in M} \operatorname{ann}(m)$$

特别地, 若是 $\operatorname{ann} M = \{0_R\}$, 称模为**忠实的 (faithful)**.

例 1.3.22. 下面给出挠模的一些例子:

(1) 有限 Abel 加群必有对其任意非零元素 $x \neq 0$, 存在 $m \in \mathbb{Z}$, 使得 $m \neq 0, m.x = 0$(也就是这是个左 $\mathbb{Z}-$ 模). 其模的零化子为 $m\mathbb{Z}$.

(2) 设域 k 上线性空间 V 上的线性变换 A, $k[x]$ 为域 k 一元多项式环. 在前文可知对 V 构造出一个 $k[x]-$ 模的模结构. 注意到 V 的挠率 $\operatorname{ann}(V)$ 本身是主理想整环 $P[X]$ 的一个理想. 设 $q(x)$ 为 A 的极小多项式, 则其生成的主理想 $\langle q(x) \rangle$ 即为 $\operatorname{ann}(V)$.

定理 1.3.23 (零化子的性质). *设 $R-$ 模 M,*

(1) 挠率 $\operatorname{ann}(M)$ 为环 R 的双边理想.

(2) 令 $(r + \operatorname{ann}(M)).m = rm$, 由此诱导出一个 $R/\operatorname{ann}(M)$ 上的模结构, 此模是是忠实的.

证明. (1) $\operatorname{ann}(M)$ 是 R 的子模. 事实上, 它也是 R 的一理想. 只是我们不能确定它是否为双边理想. 考虑任意 $r, r' \in R$ 和 $a \in \operatorname{ann}(M), m \in M$, 直接验算如下:

$$(rar').m = ra.(r'm) = (ra).(m') = r.(am') = r.0 = 0$$

由此得 $R\operatorname{ann}(m)R \subseteq \operatorname{ann}(m)$, 于是 $\operatorname{ann}(m)$ 构成双边理想.

(2)

$$\begin{aligned} r + \operatorname{ann}(M) = r' + \operatorname{ann}(M), r \neq r' &\iff r - r' \in \operatorname{ann}(M) \\ &\iff (r - r').m = 0, m \in M \\ &\iff r.m = r'.m \end{aligned}$$

这说明了良定义的. 直接验证可知 M 关于此运算构成 $R/\operatorname{ann}(M)$ 模, 以及记 $\operatorname{ann}(M) = A$.

$$(x + A)m = 0 \iff x + A \in \operatorname{ann}_{R/A}(M) \iff xM = 0 \iff x \in A$$

由此 R/A 中只有零元素零化 R, 此时 M 忠实的.

□

例 1.3.24. k 是一个域, 设 V, W 为两个 $k-$ 模, 所有 $k-$ 线性同态 $\sigma : V \to W$ 构成的集合记作 $\mathrm{Hom}_k(V, W)$. 考虑任意的 $\sigma, \tau \in \mathrm{Hom}_k(V, W)$, 关于同态的逐点相加的运算 $\sigma + \tau$. 对任意的 $x \in K, v \in V, xv \in V$, 我们有:

$$\begin{aligned}(\sigma+\tau)(xv) &= \sigma(xv) + \tau(xv)\\ &= x\sigma(v) + x\tau(v)\\ &= x(\sigma(v) + \tau(v))\\ &= x((\sigma+\tau)v)\end{aligned}$$

于是 $\sigma + \tau \in \mathrm{Hom}_K(V, W)$, 从而 $\mathrm{Hom}_K(V, W)$ 构成 Abel 群, 单位元为恒定映射. 更一般的, 如果 k 是交换环, 则 $\mathrm{Hom}_k(V, W)$ 可构成 $k-$ 模结构. 这是因为对任意的 $v \in V, x, y \in K, x\sigma \in \mathrm{Hom}_K(V, W)$ 有:

$$\begin{aligned}x\sigma(yv) &= x(y\sigma(v))\\ &= xy(\sigma(v))\\ &= yx(\sigma(v))\\ &= y(x\sigma(v)\end{aligned}$$

从而, $x\sigma \in \mathrm{Hom}_k(V, W)$, 即其关于 k 上数乘封闭. 特别地, 当 $V = W$ 时, $\mathrm{End}_k(V) = \mathrm{Hom}_k(V, W)$ 构成自同态环, 环上乘法是 $k-$ 自同态的自然合成. 上述 $k-$ 模 V 所导出的 $k-$ 自同态环 $\mathrm{End}_k(V)$ 称为**环 k 在 V 上的中心化子 (centralizer)**.

在群论中, 我们有单群的概念, 它是分类有限群的重要结构块. 类似的, 对于模论, 我们有单模的概念, 它是模的基本重要结构块.

定义 1.3.25. R 是一个环, 称一个左 $R-$ 模 M 是**单模 (simple module)**, 如果它的子模仅有 (0) 和它本身 M. 单模, 也称为**不可约模 (irreducible module)**.

例 1.3.26. 素数阶循环群 $\mathbb{Z}_p$ 是单群, 那么建立在其之上的左 $\mathbb{Z}_p-$ 模必然是单模.

定理 1.3.27 (单模的等价刻画). *$R-$ 模 M 是不可约的 (单模), 当且仅当存在 $0 \neq m \in M$ 使得 $M = \langle m \rangle$ 是循环模.*

证明. 若模 M 是循环的, 设其非零子模 $T \subset M$, 取一元素 $t \in T$, 由子模关于数乘的封闭性可知 $Rt \subset T$. 于是存在 $r' \in R$ 及 $0 \neq m \in M$, 使得 $t = r'm$. 因此, $Rt = Rr'm = Rm$. 从而

$$\langle m \rangle = \langle t \rangle \subseteq T \subseteq M = \langle m \rangle$$

故 $T = M$. 反过来, 若模 M 是不可约, 模中任意元素生成的循环子模 $\langle m\rangle = M$. M 是循环模. □

推论 1.3.28. *设 R 是个环, 左 $R-$ 模 M 是循环模, 当且仅当存在左理想 $I \subset R$, 使得 $M \cong R/I$.*

证明. M 是循环模当且仅当, $M = \langle m\rangle = Rm \cong R/\operatorname{ann}(m)$. 也就是 $I = \operatorname{ann}(m)$, 事实上这还是个双边理想. 等价关系继续有: $R/\operatorname{ann}(m)$ 是单模, 从而 $\operatorname{ann}(m)$ 是极大子模. 环 R 的理想与正则模的子模一一对应, 于是就是 $\operatorname{ann}(m)$ 极大理想. □

1.4 模上的链条件

本次讨论介绍任意环上模的链条件. 讨论目标:1. 证明 Jordan-Holder 定理 2. 介绍模上的 ACC, DCC 条件与合成列 3. 介绍左向量空间.

定理 1.4.1 (**Zassenhaus 引理**). *给定模 M(在任意环上) 的子模 $A \subseteq A^*$ 和 $B \subseteq B^*$ 存在同构:*

$$(A + (A^* \cap B^*))/(A + (A^* \cap B)) \cong (B + (B^* \cap A^*))/(B + (B^* \cap A)).$$

注 10. 下面介绍 Zassenhaus 引理关于群的版本的证明, 略加修改后即为关于模的版本的证明. Zassenhaus 引理有时也被成为蝴蝶引理, 引理中的同构在下列意义下对称: 交换左端符号 A, B 得到右端.

证明. 我们断言 $(A\cap B^*)\lhd(A^*\cap B^*)$, 即 $c \in (A\cap B^*), x \in (A^*\cap B^*)$, 则 $xcx^{-1} \in (A\cap B^*)$: 由于 $c \in A$, $x \in A^*$ 且 $A \lhd A^*$, 所以 $xcx^{-1} \in A$. 但因 $c, x \in B^*$, 所以有 $xcx^{-1} \in B^*$. 因此 $(A \cap B^*) \lhd (A^* \cap B^*)$. 有对称性同理可得, $(B \cap A^*) \lhd (A^* \cap B^*)$. 而对于子集 $D = (A \cap B^*) \lhd (A^* \cap B^*)$, 它由两个正规子群生成, 因此它也是 $A^* \cap B^*$ 的正规子群.

运用对称性, 可知只需证明同构:

$$A + (A^* \cap B^*)/A + (A^* \cap B) \cong A^* \cap B^*/D,$$

定义:

$$\varphi : A(A^* \cap B^*) \to A^* \cap B^*/D$$

$$\varphi : ax \to xD, \quad a \in A, x \in A^* \cap B^*$$

现在 φ 是良定义的, 同时还是同态. 则可以验证 φ 为满射且 $\operatorname{Ker}\varphi = A(A^* \cap B)$. 则由第一同态定理可完成证明. □

定义 1.4.2. 模 M 的一个**列 (或一个过滤 (filtration))** 是指子模的有限序列

$$M = M_0, M_1, M_2, \ldots, M_n = \{0\}$$

它满足,

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = \{0\}$$

这个列的**因子模 (factor module)** 是指模 $M_0/M_1, M_1/M_2, \ldots, M_{n-1}/M_n = M_{n-1}$, **长度 (length)** 是指严格包含关系的个数, 即非零因子模的个数.

列的一个**加细 (refinement)** 是指以原来的列作为子序列的列

$$M = M_0, M = M_1, \cdots, M = M_k = \{0\}$$

称模 M 的两个列**等价 (equivalent)**, 如果在两个非零因子模的集合间存在双射使得对应的因子模同构.

定理 1.4.3 (**Schreier 定理**). *模 M 的任意两个列*

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = \{0\}, N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k = \{0\},$$

有等价的加细.

注 11. 下面介绍 Schreier 定理的群版本证明, 稍加修改即可得到模版本的证明.

证明. 我们在第一个列的每个相邻对之间插进第二个列的一个复制. 更详细地说, 对每个 $i \geqslant$, 定义:

$$G_{ij} = G_{i+1}(G_i \cap N_j)$$

(因为 $G_{i+1} \lhd G_i$, 这是一个子群). 注意, 因为 $N_0 = G$, 所以

$$G_{i0} = G_{i+1}(G_i \cap N_0) = G_{i+1}G_i = G_i,$$

又因为 $N_k = \{1\}$, 从而

$$G_{ik} = G_{i+1}(G_i \cap N_k) = G_{i+1},$$

所以, G_{ij} 的列是 G_j 的列的子序列:

$$\cdots \geq G_i = G_{i0} \geq G_{i1} \geq G_{i2} \geq \cdots \geq G_{ik} = G_{i+i} \geq \ldots,$$

同样, 子群

$$N_{pq} = N_{p+1}(N_p \cap G_q)$$

形成第二个列的子序列. 两个新的子序列都有 nk 个项. 由 Zassenhaus 定理表(1.4.1)明, 两个子序列都是正规列, 因此是加细, 且存在同构

$$G_{i+1}(G_i \cap N_j)/G_{i+1}(G_i \cap N_{j+1}) \cong N_{j+1}(N_j \cap G_i)/N_{j+1}(N_j \cap G_{i+1}),$$

则得到两个加细等价. □

定义 1.4.4. 模的**合成列 (composition series)** 是指一切非零因子模都是单模的列.

注 12. 一个合成列只允许有无意义的加细, 也就是只能重复它的项. 精确来说, 合成列的任一加细等价于原来的合成列.

定义 1.4.5. 任意环上 R 上的一个左 R-模 M 称为有**升链条件 (ascending chain condition)**, 简写为 ACC, 如果每个左子模的升链都有终止. 称为有**降链条件 (descending chain condition)**, 简写为 DCC, 如果每个左子模的降链都有终止.

注 13. 模上链条件的等价刻画与环上链条件的等价刻画平行.

定理 1.4.6 (有限长度模的等级刻画). *任意环 R 上的模 M 有合成列当且仅当它有关于子模的两个链条件.*

证明. 如果 M 有长度为 n 的合成列, 则没有一个子模序列的长度大于 n, 否则就要违背 Schreier 定理(1.4.3), 所以 M 有两个链条件.

设 F_1 是 M 的一切真子模族, 则根据极大条件, 给出极大子模 $M_1 \in F_1$, 设 F_2 是 M_1 的一切真子模的族, 并设 M_2 是这种极大子模, 迭代可以得到递减序列.

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = \{0\}$$

其中包含关系均为真包含关系.

如果 M_n 出现在这个序列中, 则阻碍构造 M_{n+1} 的只有 $M_n = 0$. 因 M 有两个链条件, 这个链必终止, 所以有某个 t 使得 $M_t = 0$, 这个链就是 M 的合成列. □

定理 1.4.7 (Jordan—Holder 定理). *模 M 的任意两个合成列等价, 特别地, 如果合成列存在, 则合成列的长度是 M 的不变量, 叫做 M 的长度.*

证明. 由 Schreier 定理(1.4.3), 任意两个合成列等价, 特别地, 它们具有相同的长度. □

推论 1.4.8. *如果模 M 的长度为 n, 则每个模 M 的子模的链的长度小于 n.*

证明. 根据 Schreier 定理(1.4.3), 给定的链可以加细为一个合成列, 所以给定链的长度最多为 n. □

如果 Δ 是除环, 则一个左 Δ-模叫做 Δ 上的一个左向量空间. 下面的来自线性代数的定义在这里仍然有意义.

定义 1.4.9. 如果 V 是除环 Δ 上的一个左向量空间, 则 V 中的表 $X = x_1, \ldots, x_m$ 称为**线性相关 (linearly dependent)**, 如果有某个 i 使得

$$x_i \in \langle x_1, \ldots, \hat{x_i}, \ldots, x_m \rangle$$

否则称 X 为**线性无关 (linearly independent)**.

1.5 正合列

到目前为止, 我们所研究的还都是单个对象及映射, 进一步的我们将引入图和列的概念, 将研究多个对象及其态射之间的联系, 并引入序列的正合性和图的交换性, 为后续范畴论的学习打好基础. 本次重点讨论正合列的基本概念, 可裂正合列的刻画, 以及蛇引理五引理等定理的证明.

定义 1.5.1. 左 $R-$ 模 M_i 及模同态序列 $f_i \in \mathrm{Hom}(M_{i-1}, M_i)$:

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

称序列在 M_i 处**正合** (exact), 如果 $\mathrm{Im}\, f_i = \mathrm{Ker}\, f_{i+1}$. 如果对任意的 $i \in I(I$ 为指标集), 序列在 M_i 处均正合, 则称模同态序列为**正合列** (exact sequence).

例 1.5.2. 下面是一些正合列常见的例子, 以下皆为模同态序列.

(1) $0 \longrightarrow M \xrightarrow{f} M_1$ 为正合列, 当且仅当 f 为单同态.

(2) $M \xrightarrow{g} M_2 \longrightarrow 0$ 为正合列, 当且仅当 g 是满同态.

(3) 任何长正合列都可分裂为短正合列:

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

(4) 如果模同态序列 $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ 为正合列, 则 $A \cong \mathrm{Im}\, f$, $B/\mathrm{Ker}\, g = B/\mathrm{Im}\, f \cong C$.

(5) 设子模 $T \subseteq S \subseteq M$, 则 $0 \longrightarrow S/T \xrightarrow{i} M/T \xrightarrow{j} M/S \longrightarrow 0$ 为正合序列.

定义 1.5.3. 由一个称为**顶点** (vertices) 的集合 V, 和一个称为从 u 指向 v 的**箭头** (arrow)(有序对构成的集合 $\{(u,v)|u \in V, v \in V\}$) 组成的结构, 称为**有向多重图** (directed graph).

注 14. 在不同的范畴下, 有向图的含义也不相同. 有向图的顶点可以是模, 群, 环, 拓扑空间, Bananch 空间等等; 有向图的映射可以是同态, 连续映射, 算子等.

例 1.5.4. 通常, 代数中我们研究模为顶点, 以态射为箭头的有向图.

(1) $\begin{array}{ccc} X & & \\ \downarrow{\scriptstyle f} & \searrow{\scriptstyle h} & \\ Y & \xrightarrow{g} & Z \end{array}$ 有向图的箭头是单向的, 从一个顶点到另一个顶点的箭头称为**路径** (path), 相邻的箭头用态射的复合作为运算. 称一个有向图是**交换图** (commutative diagram), 如果图中任何两个顶点 A, B, 从 A 到 B 的任意路径相等. 例如, $g \circ f = h$.

(2) 设 S 和 T 都是模 M 的子模, 则下图可交换, 图的每行是正合列.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S\bigcap T & \xrightarrow{i} & S & \xrightarrow{j} & S/(S\bigcap T) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T & \xrightarrow{i} & S+T & \xrightarrow{j} & S+T/T) & \longrightarrow & 0 \end{array}$$

由之前所讨论, 我们知道: 对于左 $R-$ 模 M, N ,$\mathrm{Hom}(M, N)$ 也是左 $R-$ 模. 对此, 我们在交换环 R 上有模的正合列与模同态正合列的关系.

定理 1.5.5. *R 是一个交换环, M, N 是 R 上的模, 则关于正合性我们有以下结论:*

(1) $0 \longrightarrow N_1 \xrightarrow{u} N \xrightarrow{v} N_2 \longrightarrow 0$ 是正合列当且仅当

$0 \longrightarrow \mathrm{Hom}(M, N_1) \xrightarrow{u^*} \mathrm{Hom}(M, N) \xrightarrow{v_*} \mathrm{Hom}(M, N_2) \longrightarrow 0$ 是正合列.

(2) $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ 是正合列当且仅当

$0 \longrightarrow \mathrm{Hom}(M_2, N) \xrightarrow{\overline{g}} \mathrm{Hom}(M, N) \xrightarrow{\overline{f}} \mathrm{Hom}(M_1, N) \longrightarrow 0$ 正合.

注 15. 上述定理说明, 交换环 R 上 Hom 函子具有左正合性.

证明. (1) 和 (2) 的证明是类似的, 在这里只证明 (1).

(1) 必要性: 由正合知 u 是单射, 设 $k \in keru^*$, 则

$$u^*(k) \equiv uk = 0.$$

因为 u 是单射, 故 $k = 0$, 即 u^* 是单射. 设 $h \in \mathrm{Hom}(M, N')$, 于是:

$$u^*(h) = uh \in \mathrm{Im}(u^*)$$

由正合性, $vu = 0$. 故 $v^*(u^*(h)) = vuh = 0$. 即

$$\mathrm{Im}(u^*) \subseteq \mathrm{Ker}(v^*)$$

反之, 设 $h \in \mathrm{Ker}(v^*) \subseteq \mathrm{Hom}(M, N)$, 则 $v^*(h) = vh = 0$, 即

$$\mathrm{Im}(h) \subseteq \mathrm{Ker}(v)$$

由正合 $\mathrm{Ker}(v) = \mathrm{Im}(u)$, 而 u 是单射, 所以 $u^{-1}(h) \in \mathrm{Hom}(M, N')$ 有定义. 故:

$$h = u^*(u^{-1}h) \in \mathrm{Im}(u^*)$$

即

$$\mathrm{Ker}(v^*) \subseteq \mathrm{Im}(u^*)$$

故正合.

(2) 充分性: 取 $M = \mathrm{Ker}(u)$, $\tau : keru \to N'$ 为嵌入. 由于 $u^*(\tau) = u\tau = 0$, 故 u^* 是单射. 从而 $\tau = 0$, $\mathrm{Ker}(u) = 0$, 所以 u 是单射. 取 $M = N'$, 则:

$$vu = vu(1_{N'}) = v^*u^*(1_{N'}) = 0$$

所以 $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$. 取 $M = N'$, $\tau_1 : \ker(v) \to N$ 为嵌入, 由 $v^*(\tau_1) = v\tau_1 = 0$ 知:

$$\tau_1 \in \mathrm{Ker}(v^*) = \mathrm{Im}(u^*)$$

故存在 $h \in \mathrm{Hom}(kerv, N')$, 使得 $\tau_1 = u^*(h) = uh$. 即 $x \in \mathrm{Ker}(v)$, 且:

$$x = \tau_1(x) = uh(x) \in \mathrm{Im}(u)$$

所以:

$$\mathrm{Im}(u) = \mathrm{Ker}(v)$$

□

定理 1.5.6. *如下是模和模同态的有向图. 交换图中每行为正合序列. f 是模满同态, g 是模同构, 则存在唯一的模同构 h: $A_2 \mapsto B_2$, 使得有向图交换.*

$$\begin{array}{ccccccc} A_1 & \xrightarrow{i} & A & \xrightarrow{p} & A_2 & \longrightarrow & 0 \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ B_1 & \xrightarrow{j} & B & \xrightarrow{q} & B_2 & \longrightarrow & 0 \end{array}$$

证明. (1) 设 $a'' \in A''$, 由 P 是满射, 存在 $a \in A$ 使 $P(a) = a''$. 定义

$$h(a'') = qg(a)$$

该映射满足图的交换性, 下面验证它是同构及其唯一性.

(2) 验证良定义: 若 $u \in A, P(u) = a''$, 则 $qg(u) = qg(a)$. 因为 $P(a) = P(u)$, 则 $P(a-u) = 0$. 故 $a - u \in \mathrm{Ker}(p) = \mathrm{Im}(i)$. 所以存在 $a' \in A'$, 使得 $a - u = i(a)$. 从而:

$$qg(a-u) = qgi(a') = qjf(a') = 0$$

(3) 验证 h 的唯一性: 若还有态射

$$h' : A'' \longrightarrow B'',$$

满足 $h'p = qg$. 任取 $a'' \in A''$, 存在 $a \in A$, 使得 $pa = a''$, 从而:

$$h'(a'') = h'pa = qga = h(a'').$$

(4) 验证 h 是单射: 设 $h(a'')=0$, 则:

$$0 = ha'' = qga,$$

$$pa = a''$$

根据正合性:$ga \in \mathrm{Ker}(q) = \mathrm{Im}(j)$, 存在 $b' \in B'$, 使得 $ga = jb'$. 注意到 f 是满射, 于是存在 $a' \in A'$, 使得 $fa' = b'$, 则:

$$gia' = jfa' = jb' = ga$$

因为 g 是单射, 所以 $ia' = a$, 从而 $0 = pia' = pa = a''$.

(5) 验证 h 是满射: 设 $b'' \in B''$, 由于 q 是满射, 则存在 $b \in B$, 使得 $qb = b''$. 而 g 是满射, 故存在 $a \in A$, 使得 $ga = b$, 所以:

$$h(pa) = qga = qb = b''.$$

□

定理 1.5.7 (强形式蛇引理). *若有下面模正合列构成的交换图,*

$$\begin{array}{ccccccccc} U & \xrightarrow{a} & X & \xrightarrow{b} & Y & \xrightarrow{c} & Z & \xrightarrow{d} & W \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle \beta} \\ U' & \xrightarrow{a'} & X' & \xrightarrow{b'} & Y' & \xrightarrow{c'} & Z' & \xrightarrow{d'} & W' \end{array}$$

其中, α 是单射, β 是满射, 则有下述正合列

$$\mathrm{Ker}\, f \xrightarrow{\tilde{b}} \mathrm{Ker}\, g \xrightarrow{\tilde{c}} \mathrm{Ker}\, h \xrightarrow{\delta} \mathrm{Coker}\, f \xrightarrow{\overline{b'}} \mathrm{Coker}\, g \xrightarrow{\overline{c'}} \mathrm{Coker}\, h$$

其中, δ 称为连接同态, $\tilde{b}, \tilde{c}, \overline{b'}, \overline{c'}$, 分别由 b, c, b', c' 诱导.

证明. (1) 因为 $b'f = gb$, 知 b 将 $\mathrm{Ker}(f)$ 映到 $\mathrm{Ker}(g)$. 所以有:

$$\tilde{b} : \mathrm{Ker}(f) \longrightarrow \mathrm{Ker}(g),$$

同理有:

$$\tilde{c} : \mathrm{Ker}(g) \longrightarrow \mathrm{Ker}(h),$$

根据 $\tilde{c}\tilde{b} = 0$, 则 $\mathrm{Im}(\tilde{b}) \subseteq \mathrm{Ker}(\tilde{c})$. 其中, $\tilde{c}$ 是 c 在 $ker\,\mathrm{Ker}(g)$ 上的限制.

(2) 设 $y \in \mathrm{Ker}(\tilde{c}) \subseteq \mathrm{Ker}(g) \subseteq Y$, 则:

$$y \in \mathrm{Ker}(c) \cap \mathrm{Ker}(g),$$

故 $y \in \mathrm{Im}(b)$. 即存在 $x \in X$, 使得 $y = bx$. 所以:

$$b'f(x) = gbx = gy = 0$$

故 $f(x) \in \mathrm{Ker}(b') = \mathrm{Im}(a')$. 于是, 存在 u' 使得:

$$f(x) = a'u' = a'\alpha u = fau$$

从而 $f(x - au) = 0$. 即 $x - au \in \mathrm{Ker}(f)$. 所以:

$$b(x - au) = bx - bau = bx = y$$

即 $y \in \mathrm{Im}(\tilde{b})$. 故 $\mathrm{Im}(\tilde{b}) = \mathrm{Ker}(\tilde{c})$.

(3) 由 $b'f = gb$, 知 b' 将 $\mathrm{Im}(f)$ 映到 $\mathrm{Im}(g)$. 所以有

$$\overline{b'} : X'/imf \longrightarrow Y'/img$$

同理有:

$$\overline{c'} : Y'/img \longrightarrow Z'/imh$$

因为 $c'b' = 0$, 知 $\overline{c'}\,\overline{b'} = 0$. 所以 $\mathrm{Im}(\overline{b'}) \subseteq \mathrm{Ker}(\overline{c'})$.

(4) 设 $\overline{y'} \in \mathrm{Ker}(\overline{c'})$, 下面要证存在 $\overline{x'}$, 使得 $\overline{y'} = \overline{b'}\overline{x'}$, 其中 $y' = b'x', c'y' \in \mathrm{Im}(h)$. 设 $c'y' = h(z)$, 我们有如下等式:

$$0 = d'c'y' = d'h(z) = \beta d(z),$$

而 β 是单射, 从而 $d(z) = 0$. 故 $z \in \mathrm{Ker}(d) = \mathrm{Im}(c)$. 注意到 $z = cy$, 所以 $c'y' = hcy = c'gy$, 且 $c'(y' - gy) = 0$. 故:

$$y' - gy = b'x' \in \mathrm{Ker}(c') = \mathrm{Im}(b').$$

所以 $y' = b'x' + gy$. 于是 $\overline{y'} = \overline{b'}\overline{c'}$. 故 $\mathrm{Ker}(\overline{c'}) = \mathrm{Im}(\overline{h'})$.

(5) 下面说明连接态射 $\delta : \mathrm{Ker}(h) \longrightarrow \mathrm{Coker}(f)$ 的存在性. 设 $z \in \mathrm{Ker}(h)$,

$$\beta d(z) = d'h(z) = 0$$

由 β 是单射, $d(z) = 0$, 得: $z \in \mathrm{Ker}(d) = \mathrm{Im}(c)$ 所以存在 $y \in Y$ 使 $z = c(y)$. 故 $c'g(y) = hc(y) = 0$, 从而:

$$g(y) \in \mathrm{Ker}(c') = \mathrm{Im}(b')$$

于是存在 $x' \in X'$, 使 $g(y) = b'x'$. 定义:

$$\begin{aligned} \delta : \mathrm{Ker}(h) &\longrightarrow \mathrm{Coker}(f) \\ z &\longrightarrow x' + \mathrm{Im}(f) \end{aligned}$$

其中 x' 由 $y \in Y$ 决定, 其中 $y \in Y$ 满足 $b'x' = g(y)$, $z = cy$. 现证明 δ 是良定义的. 若 $\tilde{x'}$ 也满足此条件, 则 $c(y - \tilde{y}) = 0$, 故:

$$y - \tilde{y} \in \mathrm{Ker}(c) = \mathrm{Im}(b)$$

从而, 存在 $x \in X$ 使得 $y - \tilde{y} = b(x)$, 所以:

$$b'(x' - \tilde{x'}) = g(y - \tilde{y}) = gbx = b'f(x)$$

即

$$x' - \tilde{x'} - f(x) = a'u' = a'\alpha u = fa(u)$$

所以 $x' - \tilde{x'} \in \mathrm{Im}(f)$. 于是 $x' + \mathrm{Im}(f) = \tilde{x'} + \mathrm{Im}(f)$. 故 δ 是良定义的.

(6) 下面要找到 $z = cy, y \in \mathrm{Ker}(g)$. 若 $y \in \mathrm{Ker}(g), c(y) = z \in \mathrm{Ker}(h)$, 则 $gy = 0$, $hcy = c'g(y) = 0$. 所以

$$g(y) \in \mathrm{Ker}(c') = \mathrm{Im}(b')$$

因为 $gy = 0 = b'x'$, 故 $x' \in \mathrm{Ker}(b') = \mathrm{Im}(a')$, 所以:

$$x' = a'u' = a'\alpha u = fa(u) \in \mathrm{Im}(f)$$

故 $\delta z = 0$, 即 $\mathrm{Im}(\tilde{c}) \subseteq \mathrm{Ker}(\delta)$.

(7) 设 $z \in \mathrm{Ker}(\delta), z \in \mathrm{Ker}(h)$, 则 $b'x' = g(y)$, $z = cy$. 所以 $x' = f(x)$, 故:

$$g(y) = b'f(x) = gb(x)$$

从而 $y - bx \in \mathrm{Ker}(g)$, 于是:

$$c'g(y - bx) = hc(y - bx) = 0$$

所以 $g(y-bx) \in \mathrm{Ker}(c') = \mathrm{Im}(b')$, 从而 $g(y-bx) = b'\tilde{x'} = b'f(x)$, 所以 $z = c(y-bx)$.

(8) 最后证明 $\mathrm{Im}(\delta) = \mathrm{Ker}(\overline{b'})$. 因为

$$\overline{b'}\delta z = \overline{b'}(x' + \mathrm{Im}(f)) = b'x' + \mathrm{Im}(g) = g(y) + \mathrm{Im}(g) = 0$$

所以 $\mathrm{Im}(\delta) \subseteq \mathrm{Ker}(\overline{b'})$. 设 $x' + \mathrm{Im}(f) \in \mathrm{Ker}(\overline{b'})$, 即 $b'x' \in \mathrm{Im}(g)$. 从而, 存在 $y \in Y$, 使得 $b'x' = gy$. 所以 $hcy = c'gy = c'b'x' = 0$, 即 $c(y) \in \mathrm{Ker}(h)$, 且 $\delta c(y) = x' + \mathrm{Im}(f)$. 即 $x' + \mathrm{Im}(f) \in \mathrm{Im}(\delta)$.

□

定理 1.5.8 (可裂正合列的等价刻画). 设 $0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ 为模的正合列, 则以下等价:

*(1) 存在 $h \in \mathrm{Hom}(M_2, M)$, 使得 $g \circ h = 1_{M_2}$, 此时称 g 是***截断*** ***(section)***.*

*(2) 存在 $k \in \mathrm{Hom}(M, M_1)$, 使得 $k \circ f = 1_{M_1}$, 此时称 f 是***收缩*** ***(retraction)***.*

(3) 存在 $\varphi \in \mathrm{Hom}(M_1 \bigoplus M_2, M)$ 是同构, 且下图交换 (其中, t_1 是嵌入, π_2 是投影).

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{t_1} & M_1 \bigoplus M_2 & \xrightarrow{\pi_2} & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_{M_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_{M_2}} & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{f} & M & \xrightarrow{g} & M_2 & \longrightarrow & 0 \end{array}$$

我们称满足上述三个条件之一的正合列为***可分裂正合列*** ***(split exact sequence)***.

证明. (A) (1)$\Longrightarrow$ (3): 设 $(x_1, x_2) \in M_1 \oplus M_2$, 考虑:

$$\phi(x_1, x_2) = f(x_1) + h(x_2)$$

从而, $\phi \in \mathrm{Hom}(M_1 \oplus M_2, M)$, 且 ϕ 使得图交换, 由强形式蛇引理(1.5.7), ϕ 为同构.

(B) (2)$\Longrightarrow$ (3): 设 $x \in M, \omega(x) = (k(x), g(x)) \in M_1 \oplus M_2$, 所以 $\omega \in \mathrm{Hom}(M, M_1 \oplus M_2)$, 且下图交换:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f} & M & \xrightarrow{g} & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_{M_1}} & & \downarrow{\scriptstyle \omega} & & \downarrow{\scriptstyle 1_{M_2}} & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{\tau_1} & M_1 \oplus M_2 & \xrightarrow{\pi_2} & M_2 & \longrightarrow & 0 \end{array}$$

令 $\phi = \omega^{-1}$ 即可.

(C) (3) $\Longrightarrow$ (1)(2): 设 τ_2 为 M_2 到 $M_1 \oplus M_2$ 的嵌入, π_1 为 $M_1 \oplus M_2$ 到 M_1 的投影, 则令:

$$h = \phi \circ \tau_2, k = \pi_1 \circ \phi^{-1}$$

即满足条件 (1)(2).

□

最后, 我们给出一个不可裂的正合列的例子.

例 1.5.9. $0 \longrightarrow n\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$ 是一个不可分的正合列.

第二章　Zorn 引理

2.1　选择公理, 良序原则, Zorn 引理

我们一开始会介绍选择公理以及良序原则, 紧接着引出佐恩引理. 事实上这三个定义阐述的内容是等价的. 此次的重点是佐恩引理的应用—在证明交换幺环的极大理想存在性, 域上向量空间的基的存在性, 诺特环的另一等价条件等等.

公理 2.1 (**选择公理 (Choice Axiom)**)**.** *如果 A 是集合, 令 $P(A)$ 表示它的一切非空子集的族,* **选择公理***的陈述为: 如果 A 是非空集合, 则存在函数 $\beta : P(A) \to A$ 使得对 A 的每个非空子集 S, 使得 $\beta(S) \in S$. 这样的函数 β 叫做***选择函数***.*

定义 2.1.1. 以下用一个较简单的描述: **选择公理**. 设 C 为一个由非空集合所组成的集簇. 那么, 我们可以从每一个在 C 中的集合中, 都选择一个元素和其所在的集合配成有序对来组成一个新的集合.

下面我们给出偏序集的定义:

定义 2.1.2. 对于集合 S, S 中有一个偏序 $\preceq$, 对于任意的 $a, b, c \in S$; 若 S 是一个**偏序集 (partial ordered set)**, 则满足以下条件:

(1) 若 $a \preceq b, b \preceq c$; 则 $a \preceq c$.

(2) $a \preceq a$.

(3) 如果 $a \preceq b, b \preceq a$; 则 $a = b$.

定义 2.1.3. 设 X 是偏序集, 如果 X 的每个非空子集 S 包含一个最小元素; 即存在 $s_o \in S$ 使得对任意的 $s \in S$:

$$s_o \preceq s$$

则称 X 为**良序的 (well—ordered)**. 如果偏序集 X 中的任意两个元素都可以比较, 即对一切 $x, y \in X$, 或者 $x \preceq y$, 或者 $y \preceq x$, 则称 X 为**链 (chain)**.

例 2.1.4. (1) 空集是良序集; 否则, 空集将包含 (没有最小元素的) 的非空子集, 这是矛盾的.

(2) 整数集 $\mathbb{Z}$ 不是良序集, 因为没有最小整数.

(3) 定义 $\mathbb{Q}$ 的子集 X 为: $X = \{1 - \frac{1}{n} : n \geq 1\} \cup \{2 - \frac{1}{n} : n \geq 1\}$; 则 X 是良序集. 注意 $1 = 2 - \frac{1}{1}$ 有无限个前导.

性质 2.1.5. *下面是良序集的几个基本性质:*

(1) 良序集 X 的每个子集 Y 也是良序集.

(2) 设 X 是良序集, 如果 $x, y \in X$, 则 $x \preceq y$ 或者 $y \preceq x$.

(3) 如果 X 是良序集, 则 X 中的每个严格递减序列 $x_1 \succeq x_2 \succeq x_3 \succeq \cdots$ 是有限的.

证明. (1) 如果 S 是 Y 的非空子集, 则它也是 X 的子集, 并且和 X 的任意非空子集一样, 它包含了最小元素, 所以 Y 是良序集.

(2) 子集 $S = \{x, y\}$ 有最小元, 它或者是 x, 或者是 y. 则必有 $x \preceq y$ 或者 $y \preceq x$.

(3) 如果 X 是良序集, 则 $S = \{x_1, x_2, \cdots\}$ 有最小元素, 比如 x_i; 即对一切 $n \geq 1, x_n \succ x_i$. 特别的, 如果 $n = i + 1$, 则 $x_{i+1} \succ x_i$, 这与 $x_i \succ x_{i+1}$ 矛盾.

□

公理 2.2. 良序原则 ***(well ordered principal)****: 每个集合 X 都可以良序化.*

例 2.1.6. $\mathbb{Z}$ 可以这样良序化:

$$0 \preceq 1 \preceq -1 \preceq 2 \preceq -2 \preceq 3 \preceq -3 \cdots$$

定义 2.1.7. 设 X 是偏序集, X 的子集 S 的一个**上界 (upper bound)** 是指元素 $x \in X$, 不必在 S 中, 满足对一切 $s \in S, s \preceq x$. 如果对于元素 $m \in X$, 没有 $x \in X$ 满足 $m \prec x$; 即如果 $x \in X$ 并且 $m \preceq x$, 则 $m = x$, 则称 m 为一个**极大元 (maximal element)**.

注 16. 一个偏序集可以没有极大元素: 例如 $\mathbb{R}$ 在通常序列下是一个链, 但它没有极大元素. 一个偏序集也可以有很多个极大元素: 例如 X 是集合 U 的一切真子集构成的偏序集, 则子集 S 是极大元素当且仅当有某个 $u \in U$ 使得 $S = U - \{u\}$; 即 S 是一个点的补集.

从上述定义中自然的一个问题是偏序集的极大元是否总是存在. 有了以上的准备, 我们可以陈述 Zorn 引理回答这个问题.

公理 2.3 (Zorn 引理). *若 S 是偏序集, 且对 S 上任意一条链 T; T 有上界, 则 S 中存在极大元素.*

定理 2.1.8 (ZFC 公理体系). *下列陈述等价:*

(1) Zorn 引理

(2) 良序原则

(3) 选择公理

定理 2.1.9. 如果 C 是链且 $S=\{x_1,x_2,x_3,\cdots\}\subseteq C$, 则存在某个 x_i, 其中 $1\leq i\leq n$, 使得对一切 $x_j\in S$ 有 $x_j\preceq x_i$.

证明. 对 $n\geq 1$, 用归纳法证明. 初始步显然为真, 设 $S=\{x_1,x_2,\cdots x_{n+1}\}$, 并定义 $S'=\{x_1,x_2,\cdots x_n\}$. 归纳假设给出 x_i, 其中 $1\leq i\leq n$, 使得对一切的 $x_j\in S'$, 有 $x_j\preceq x_i$. 因为 C 是链, 所以 $x_i\preceq x_{n+1}$ 或者 $x_{n+1}\preceq x_i$. 两种情形都给出了 S 中的极大元素. □

性质 2.1.10. 如果 R 是非零交换环, 则 R 有极大理想. 事实上, R 中的每个真理想 I 都包含在一个极大理想中.

证明. 首先因为 R 是非零环, 所以理想 $\{0\}$ 是真理想, 从而存在 R 中的极大理想包含它. 设 X 是包含了 I 的一切真理想的族 (注意, 因为 $I\in X$, 所以 $X\neq\varnothing$), 用包含作为集合的偏序. 易知 X 的极大元素是 R 中的极大理想. 设 $\mathcal{C}$ 是 X 的一条链, 于是给定 $I,J\in\mathcal{C}, I\subseteq J$ 或者 $J\subseteq I$. 我们断言:

$$I^*=\bigcup_{I\in\mathcal{C}I}$$

I^* 是 $\mathcal{C}$ 的一个上界. 显然对一切 $I\in\mathcal{C}, I\subseteq I^*$. 所以只要证明 I^* 是真理想. 容易验证得 I^* 是理想. 又如果 $I^*=R$, 则 $1\in I^*$. 1 取自 I^* 必有 $I\in\mathcal{C}$ 使得 $1\in I$, 这与 I 是链 $\mathcal{C}$ 中的真理想矛盾, 从而则命题得证. □

注 17. 如果环 R 的定义中没有包含 1, 则上述命题不一定成立. 但任何一个不含单位的环都可以作为一个理想嵌入到含幺环中. 因此, 我们只需要研究含幺环即可.

定义 2.1.11. 设 V 是某个域 k 上的向量空间, 并设 $Y\subseteq V$ 是一个无限子集.

(1) 称 Y **线性无关**, 如果 Y 的每个有限子集线性无关.

(2) 称 Y **张成 (span)**V, 如果每一个 $v\in V$ 是 Y 中有限个元素的线性组合. 当 V 由 Y 张成时, 记 $V=\langle Y\rangle$.

(3) 向量空间 V 的一组**基 (basis)** 是指一组张成 V 的线性无关的子集. 由此, 一个无限子集 $Y=\{y_i:i\in I\}$ 线性无关, 如果一旦 $\sum a_iy_i=0$, 则一切 $a_i=0$.

例 2.1.12. 设 k 是域, 并把 $V=k[x]$ 看作 k 上的向量空间, 我们断言:

$$Y=\{1,x,x^2,\cdots x^n,\cdots\}$$

是 V 的一组基, 因为任意一个 d 次多项式是 $1,x,x^2,\cdots x^d$ 的线性组合, 所以 Y 张成 V. 因为不存在不全为 0 的标量 $a_0,a_1,a_2,\cdots a_n$ 满足 $\sum\limits_{i=0}^{n}a_ix^i=0$. 所以 Y 也线性无关, 因此 Y 是 V 的基.

引理 2.1.13. 设 R 是交换环, 并设 $\mathcal{F}$ 是 R 中一切非有限生成理想的族, 如果 $\mathcal{F} \neq \varnothing$, 则 $\mathcal{F}$ 有极大理想.

证明. 用包含作为 $\mathcal{F}$ 的偏序, 根据 Zorn 引理, 只要证明: 如果 $\mathcal{C}$ 是 $\mathcal{F}$ 中的链, 则:

$$I^* = \bigcup_{I \in X} I$$

不是有限生成的. 反之, $I^* = (a_1, a_2, \cdots a_n)$, 则有某个 $I_j \in \mathcal{C}$, 使得 $a_j \in I_j$. 又因为 $\mathcal{C}$ 是链, 则理想 $I_1, I_2, \cdots In$ 中有一个包含其他各个理想, 记为 I_0. 从而 $I^* = (a_1, a_2, \cdots a_n) \subseteq I_0$. 因为对所有的 $I \in \mathcal{C}$, 有 $I \subseteq I^*$, 所以反包含 $I_0 \subseteq I^*$ 是显然的. 于是 $I_0 = I^*$ 是有限生成的, 这与 $I_0 \in \mathcal{F}$ 矛盾. □

定理 2.1.14. 交换环 R 是诺特环, 当且仅当 R 中的每个素理想都是有限生成的.

证明. 由诺特环的等价条件知必要性显然, 只需证明充分性. 假定每个素理想都是有限生成的. 令 $\mathcal{F}$ 是 R 中一切非有限生成的理想的族, 如果 $\mathcal{F} \neq \varnothing$, 则根据 Zorn 引理有一个 $\mathcal{F}$ 中的极大理想 I. 我们要证明 I 是素理想, 从而和假设每个素理想都是有限生成的矛盾, 因此 $\mathcal{F} = \varnothing$. 即 R 是诺特环. 假设 $ab \in I$ 而 $a \notin I$ 且 $b \notin I$. 因为 $a \notin I$, 则 $I + Ra$ 严格大于 I, 从而 $I + Ra$ 是有限生成的. 于是可以假定:

$$I + Ra = (i_1 + r_1 a, i_2 + r_2 a, \cdots, i_n + r_n a)$$

其中对一切 $k, i_k \in I, r_k \in R$. 考虑 $J = (I : a) = \{x \in R : xa \in I\}$. 现在,

$$I + Rb \subseteq J((i_k + r_k b) \in I)$$

又因为 $b \notin I$, 显然有 $I \subset J$, 从而 J 是有限生成的. 我们断言:

$$I = (i_1, i_2, \cdots, i_n, Ja)$$

因为每个 $i_k \in I$ 和 $Ja \subseteq I$, 显然有 $(i_1, i_2, \cdots, i_n, Ja) \subseteq I$. 关于反包含, 如果 $z \in I \subseteq I + Ra$, 则存在 $u_k \in R$, 使得:

$$z = \sum_k u_k (i_k + r_k a)$$

于是:

$$\sum_k u_k r_k) a = z - \sum_k u_k i_k \in I$$

从而 $\sum\limits_k u_k i_k \in J$, 因此:

$$z = \sum_k u_k i_k + \left(\sum_k u_k r_k \right) a \in (i_1, i_2, \cdots, i_n, Ja)$$

由此, $I = (i_1, i_2, \cdots, i_n, Ja)$ 是有限生成的, 产生矛盾, 从而 I 是素理想.

□

2.2 自由模 (一)

主要是有关自由模的一些性质.

定义 2.2.1. 我们称 K-模为其子模 V_γ 的**内直和 (inner direct product)**, 若:

$$V = \sum_{\gamma\in\Gamma} V_\gamma$$

$$V_i \cap \sum_{\gamma\neq i} V_\gamma = 0, \forall i \in \Gamma$$

即 V 中元素可唯一表述成 $\sum\limits_{i=1}^{n} v_i, v_i \in V_i$, 此时又可以记作:

$$V = \bigoplus_{\gamma\in\Gamma} V_\gamma$$

称 K-模为一系列的 V_γ 模的**外直和 (exterior direct product)**, 是由笛卡尔积 $\prod\limits_{\gamma\in\Gamma} V_\gamma$ 中仅有有限个不为 0 的坐标分量构成的集合. 即对任意的 $a = (a_\gamma) \in \prod_{\gamma\in\Gamma} V_\gamma$, a 的支撑集:

$$\mathrm{Supp}(a) = \{\gamma \in \Gamma \mid a_\gamma \neq 0\}$$

有限. 此时称作模的外直和, 并定义运算关系:

$$(a_i) + (b_i) = (a_i + b_i)$$

$$k(a_i) = (ka_i), k \in K$$

性质 2.2.2. *模的内, 外直和其实本质是一回事, 至少在同构意义下一致.*

对此可以考虑投影映射 $(a_i) \mapsto a_i$, 此引发外直和到其直和因子 S_i 上的同态, 故而有同态 $f(a) = \sum a_i$, 由于内直和在涉及每个分量上表述唯一, 也就是逆映射存在, 故而是构成同构. 反过来对于映射 $a_i \mapsto (\ldots 0, 0, a_i, 0, \ldots)$(对于 i 可数下, 可以写成左边元组形式, 不可数也无伤大碍), 由此构成一个集合:

$$S_i \cong S_i' = \{(\ldots 0, 0, a_i, 0, \ldots)\}$$

显然 $\oplus S_i$ 形成一种外直和. 其中, 对于 i 有限下, 外直和与笛卡尔积无任何区别, 但当变成无限情况, 外直和是为笛卡尔积的一个子集.

定理 2.2.3. *设 $S_i, i \in I, D, M$ 为左 R-模, $D = \bigoplus S_i$, 设 j_i 为一般的嵌入同态映射, 若给出 R-同态映射族 $\{f_i, i \in I : S_i \to M\}$, 则唯一指定同态映射 $\theta : D \to M$ 使得如下交换图成立:*

$$\begin{array}{ccc} S_i & & \\ \downarrow{\scriptstyle j_i} & \searrow^{f_i} & \\ D & \xrightarrow{\theta} & M \end{array}$$

证明. 先考虑存在性. 对 $a \in D$, 由于 D 是直和, 故 $a =$(其中 s_i 准确来说是 $j_i(s_i), s_i \in S_i$, 但这么写完全可以理解) 之后取映射 $\theta(a) = \theta(\sum\limits_{finite} s_i) = \sum\limits_{finite} f_i(s_i)$. 显然这是个模同态, 且使得交换图交换. 唯一性可以考虑新的让交换图交换的同态 $\gamma : D \to M$. 由:

$$\gamma(a) = \gamma(\sum s_i) = \sum f_i(s_i) = \theta(a)$$

可知唯一. □

定理 2.2.4. 设 M_i 为左 R-模, S_i 为其子模, i 属于某指标集 I, 则如下模同构成立:

$$\frac{\bigoplus_i M_i}{\bigoplus_i S_i} \cong \bigoplus_i \frac{M_i}{S_i}$$

证明. 思路是先考虑同态再使用第一同构定理. 构造自然同态 $\sigma_i : M_i \to M_i/S_i$, 再构造自然嵌入同态 $f_i : M_i/S_i \to \bigoplus_i \frac{M_i}{S_i}$, 此时同态的符合构成的同态构成 $f_i\sigma_i : M_i \to \bigoplus_i \frac{M_i}{S_i}$, 由此确定唯一同态 $\theta : \bigoplus_i M_i \to \bigoplus_i \frac{M_i}{S_i}$ 计算其核可以显然得知 $\ker\theta = \bigoplus_i S_i$, 由此第一同构定理给出:

$$\frac{\bigoplus_i M_i}{\bigoplus_i S_i} \cong \bigoplus_i \frac{M_i}{S_i}$$

□

定义 2.2.5. 若加群 F 与下直和同构:

$$F \cong \oplus_{i\in I}\langle x_i\rangle$$

其中要求 $\langle x_i\rangle$ 为无限循环群 (即无挠, 无非零的有限阶元素). 则称 F 为**自由 Abel 群**, 而 $\{x_i\}$ 可以称作为 F 的**基 (basis)**.

我们可以考察有限以及 $x_i \in F$ 的情况以获得些许直观, 这意味着所有 F 中的元素都可唯一写成形如 $n_1x_1 + \ldots + n_mx_m$ 的形式, 其中 $n_i \in \mathbb{Z}$. 类似向量空间的坐标, 而我们也很容易看出同构:

$$\langle x_i\rangle \cong \mathbb{Z}$$

$$F = \oplus\langle x_i\rangle \cong \mathbb{Z}^m$$

所以有时我们干脆把自由 Abel 群 F 记作 $\mathbb{Z}^m$

性质 2.2.6. $\mathbb{Z}^n \cong \mathbb{Z}^m$ 当且仅当 $m = n$

证明. 先约定一个记法:

$$mG = \{mg : g \in G\}, m \in \mathbb{Z}$$

右推左显然. 对于左推右, 考虑:

$$G = G_1 \oplus \cdots \oplus G_n, 2G = 2G_1 \oplus \cdots \oplus 2G$$

对其作商有:

$$G/2G \cong (G_1/2G_1) \oplus \cdots \oplus (G_n/2G_n)$$

取 $G_i = \mathbb{Z}$,$\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$, 且 $\underbrace{\mathbb{F}_2 \oplus \cdots \oplus \mathbb{F}_2}_{n}$ 的阶是 2^n, 若是 $\mathbb{Z}^n \cong \mathbb{Z}^m$, 有 $2^n = 2^m$, 由此 $n = m$. □

对于基成员有限的自由 Abel 群 F, 设其基的个数为 n. 则有 $F \cong \mathbb{Z}^n$. 若是我们找到另一组基, 基的个数为 m, 借助上述性质, 可以得 $n = m$. 即基的个数对于 F 是不变量. 此时仿照线性空间, 我们称作**秩 (rank)**, 记作 $\operatorname{rank} F = n$.

仿照自由群, 我们可以给出自由模的定义:

定义 2.2.7. 设左 R-模 F, 若其同构于一系列的循环 R-模的直和, 并且这些循环模是无挠的:

$$F \cong \oplus_i \langle x_i \rangle, \langle x_i \rangle \cong R$$

此时 $x_i : i \in I$ 同样可称作基. 对于有限直和情况, 不难看出 $F \cong R^n$.

特别留意的是, 自由 Abel 群其实也就是 $\mathbb{Z}$-模, 这里推广到了一般的环上. 比较遗憾的且惊奇的是形如 "$\mathbb{Z}^n \cong \mathbb{Z}^m$ 当且仅当 $m = n$" 该命题对于一般的环 R 却未必成立. 这点可以考察一般的数域 k 上的无限维线性空间 V, 取其自同态环 $\operatorname{End}_k V$ 为 R. 由此关于自身构成左 R 模. 对于无穷维线性空间 V, 我们总是可以作一个直和分解:$V = V_1 \oplus V_2$, 从而任意自同态映射的像可唯一写成形如:

$$f(x) = x_1 + x_2, x \in V_1, X_2 \in V_2$$

由此 f 可分解为:

$$f = f_1 + f_2, \text{其中 } f_1 : V \to V_1, f_2 \to V_2$$

此时注意到 $(f_1, f_2) \in R \times R$, 由此诱导映射 $R \to R \times R$.

性质 2.2.8. *对于交换含幺环 R,$R^n \cong R^m$ 当且仅当 $m = n$*

证明. 作为交换含幺环 R, 必然存在一个极大理想 M, 此时商环 R/M 构成一个域. 其次, 我们考虑一个自由 R-模:

$$V = \langle x_1, \ldots, x_n \rangle$$

其中 $\{x_1, \ldots, x_n\}$ 为基. 注意到 MV 构成 V 的一个子模, 由此诱导出商模:

$$V/MV = \{v + MV : v \in V\}$$

该商模是 R-模, 但我们可以在此建立 R/M-模, 定义为:

$$(r+M)(v+MV)=rv+MV, r+M\in R/M$$

此时不难看出定义在域上的模构成向量空间, 以及他们的基为:

$$\{\overline{x_1},\dots,\overline{x_n}\},\overline{x_i}=x_i+MV$$

由此 $V/MV\cong(R/M)^n$. 若假设另外有个基 $\{y_1,\dots,y_m\}$, 由此仿照上面会有 $V/MV\cong(R/M)^m$. 对于向量空间而言此时 $m=n$ 是显然的, 或者仿照上面 $\mathbb{Z}$ 的证明是类似的. □

定理 2.2.9 (自由性质 (Freeness Property)). *设 R 为一个环,F 是个自由左 R-模, 设 X 是 F 的一组基. 再设另一个 R-模 M. 此时若有映射 $\gamma:X\to M$, 则将存在唯一同态映射 $h:F\to M$, 且使得下图交换:*

$$\begin{array}{ccc} F & & \\ {\scriptstyle i}\uparrow & \searrow^{h} & \\ X & \xrightarrow{\gamma} & W \end{array}$$

其中 i 为一般嵌入. 交换意味着对于 $x\in X, h(x)=\gamma(x)$.

证明. 特别注意的是这里 $\gamma:X\to M$ 只是一般映射, 不是什么同态. 所以我们考虑 $\langle x_i\rangle, x_i\in X$, 显然有 $F=\bigoplus_i\langle x_i\rangle$. 考虑模同态 $f_i:rx_i\mapsto r\gamma(r)$, 此时构成 $\langle x_i\rangle$ 到 M 的同态映射, 由此确定了唯一同态映射 $h:F\to M$ □

性质 2.2.10. *设一环 R, 对于任意左 R-模 M,M 可以表示为某自由 R-模 F 的商模 (与一商模同构). 且若 M 有限生成当且仅当可以选取一个有限生成的 F*

证明. 不妨取 $F=\bigoplus_{i\in M}\langle x_i\rangle$, 也即是 $|M|$ 个 R 的" 复制". 于是 $\{x_i:i\in M\}$ 构成一组基. 考虑映射 $\gamma(x_m)=m$, 由此确定了基到 M 的映射, 进而确定唯一同态 $\theta:F\to M$, 根据第一同构定理(1.3.14)给出:

$$M\cong F/\ker\theta$$

若 $M=\langle m_1,\dots,m_n\rangle$ 是有限生成, 则上述构造的 $F=\bigoplus_{i=1}^{n}\langle x_i\rangle$ 是有限的. 反之若是 F 有限, 上述的同态映射 γ 下的像变为 M, 自然是有限的. □

性质 2.2.11. *设 R 是一个环, B 是左 R-模 A 的子模, 若商模 A/B 是自由的, 那么 B 就有一个补 C, 即满足 $A=B\oplus C, C\cong A/B$.*

证明. 考虑短正和列:

$$0 \to B \xrightarrow{i} A \xrightarrow{\sigma} A/B \to 0$$

其中 i 为嵌入, σ 为自然同态. 考虑映射:

$$f : A/B \to A; a + B \mapsto a$$

此时 σf 复合成 A/B 上的恒等映射. 由此, 该短正合列可分, 此时便有:

$$A = \operatorname{Im} i \oplus \operatorname{Im} f = B \oplus C, C \cong A/B$$

□

性质 2.2.12. *对于一个 Abel 群 A 而言, 设 X 为其一子集, 若 X 关于 A 满足自由性质 (也就是给定映射 $f : X \to G$, G 为任意一 Abel 群, 将唯一确定同态 $r : A \to G$, 使得前文的交换图成立), 那么 X 便是 A 的一个基.*

证明. 考虑 X 的一个复制, 即有集合 Y 以及双射 $p : X \to Y$, 并设其逆映射为 $q : Y \to X$. 先令 Y 自由生成一个 Abel 群 F, $k : Y \to F, j : X \to A$ 为相应的嵌入. 我们的思路显然是要说明 $A \cong F$. 给出如下交换图加以说明:

$$\begin{array}{ccc} A & & F \\ {\scriptstyle j}\uparrow & & \uparrow{\scriptstyle k} \\ X & \underset{q}{\overset{p}{\longleftrightarrow}} & Y \end{array}$$

在图中首先从 Y 出发, 映射 jp 给出 Y 到 A 的映射, 而 Y 是 F 的基, 根据自由性质可得出唯一同态 $h : F \to A$ 反过来, 我们的命题前提假设了 X 具有自由性质, 也就是存在唯一同态 $g : A \to F$. 下面再考虑如下交换图:

$$\begin{array}{ccc} A & & \\ {\scriptstyle j}\uparrow & \searrow^{hg} & \\ X & \xrightarrow{j} & A \end{array}$$

由自由性质可知存在唯一自同态 $A \to A$, 可是单位自同态也是自同态, 也满足交换图的交换性质, 由此根据同态的唯一性我们只能有 $1_A = hg$. 同理也会有 $1_F = gh$. 这就反应了 h, g 互为逆映射, 由此 $A \cong F$, 那么 F 的基 Y 对应过去便是 A 的基 X. □

一个自然的问题是: 自由模的子模是否是自由模, 这源于向量空间的子空间仍然是向量空间的一种推广, 但遗憾的是对于任意环 R 上的模, 这点未必成立. 一个例子是考虑:

$$K = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$$

K 的阶是 6, 环 K 关于自身构成的模. 其有子模:

$$2K = \{\overline{0}, \overline{2}, \overline{4}\}$$

$$3K = \{\overline{0}, \overline{3}\}$$

他们的阶分别是 $2, 3$. 若是 K-子模 $2K$ 为自由的, 这必然意味着其同构与某 K^n, 也就是它的阶必须为形如 6^n 的形式, 容易验证这是不正确.

下面的定理说明主理想环上的自由模的子模是自由的:

定理 2.2.13 (PID 上自由模的子模是自由模). *若 R 为主理想整环, 则 R-模 M 里的子模 H 是自由的.*

证明. 既然 M 是自由的, 那么就会有组基 $X = \{x_i : i \in I\}$. 对于指标集 I 而言, 良序原则给出一种排序, 在这个排序下 I 是良序的. 选择这个序 "$\preceq$" 给出集合:

$$F'_k = \{x_i : i \prec k\}\ ;\ F_k = \{x_i : i \preceq k\}$$

$$H'_k = H \cap F'_k\ ;\ H_k = H \cap F_k$$

按上述定义自然有 $H'_k = H \cap F'_k = H \cap F_k \cap F'_k = H_k \cap F'_k$, 之后考虑作商:

$$H_k/H'_k = (H_k)/(H_k \cap F'_k) \cong (H_k + F'_k)/F'_k \subseteq F_k/F'_k \cong R$$

由此上方式子很清楚的说明了 H_k/H'_k 同构于 R(作为关于自身的模而言) 的子模, 由于 R 是主理想整环, 意味着子模都是一个元素生成的循环模, 由此 $H_k/H'_k = \langle h_k + H'_k\rangle$, 由此 $H_k = \langle h_k\rangle \oplus H'_k$. 设 $H^* = \langle h_k : k \in I\rangle$, 下证 $H = H^*$. 考虑映射 $\mu : H \to I$:

$$\mu(h) = \min\{k \in I : h \in F_k\}$$

其中, 特别地 $h \in H'_k \subseteq F'_k = \cup F_i$, 进而存在 $a \prec k, h \in F_a$, 由此必然有 $\mu(h) \prec k$. 考虑 $\mu(H - H^*) \subseteq I$, 由于 I 的良序性, 这个集合是有最小元的, 设其为 j, 对应的有 $h' \in H - H^*$ 使得 $\mu(h') = j$. 此时 $h' \in H \cap F_j = H_j = \langle h_j\rangle \oplus H'_j$, 由此导出:

$$h' = rh_j + h'_j$$

上式中, 回忆 $h' \notin H^*$ 这就导致 $h'_j \notin H^*$. 否则 $h' \in H^*$. 而 $h'_j \in H'_j$, 这点意味着 $\mu(h'_j) \prec j$, 而 $h'_j \in H - H^*$, 这与 j 的最小性矛盾. 由此 $H = H^*$. 断言: H 的生成集 $\{h_k : k \in I\}$ 是线性无关的. 考察生成集的任意有限子集, 并对其合理排序使得序列 $\{h_{k_1}, h_{k_2}, \ldots, h_{k_n}\}$ 满足 $k_1 \prec k_2 \prec \cdots \prec k_n$, 再考虑方程:

$$r_1 h_{k_1} + \ldots + r_n h_{k_n} = 0$$

由 $r_n h_{k_n} = -\sum_{i=1}^{n-1} r_i h_{k_i} \in H'_{k_n}$, 进而 $r_n h_{k_n} \in H'_{k_n} \cap \langle h_{k_n}\rangle = 0$, 给出 $r_n = 0$, 递归地得到所有系数为零, 从而 H 线性无关. □

2.3 半单模、半单环及半单代数 (一)

本节内容主要涉及: 半单模的定义和等价刻画; 半单环的刻画; 半单环具体的例子; Weddernburn—Artin 定理; 证明 Maschke 定理, 它是表示论基本定理之一; 提及 Molien 定理, 并且给出一个例子: 具有同构的复群代数的非同构有限群.

半单性是重要的代数性质. 例如, 我们所熟悉的半单矩阵是可对角化矩阵; 半单线性变换是最小多项式互不相同的线性变换. 半单性的研究, 可进一步参考结合代数 (associative algebra) 的教材, 古典的结合代数理论更多关注一些低维条件下的代数分类, 比如半单代数的分类; 现代的结合代数理论更多关注一些特定的结合代数表示论和非交换几何, 比如箭图代数 (quiver algebra), Hochschild 同调/上同调 (homology/cohomology), Calabi-Yau 完备化等.

单模 (simple module), 又称为不可约模 (irreducible module); 半单模 (semisimple module), 又称为完全可约模 (completely reducible module). 我们指出: 研究一个半单模的结构, 实际上就是研究这个完全可约模的所有不可约子模的结构, 从而归结为单模的研究. 我们有必要讨论一类重要的环: 半单环. 半单环囊括了大部分群代数 kG.

2.3.1 半单模

定义 2.3.1. R 是一个环, 称左 $R-$ 模 M 为**单模**, 若 $M \neq 0$ 且 M 无非平凡的子模. 称 M 为**半单模**, 若 $M = \bigoplus\limits_{i\in I} M_i$, $\forall i \in I$, M_i 是单模.

注 18. (a) $\{0\}$ 模不是单模, 但其为半单模; 这是因为 $\{0\} = \bigoplus\limits_{i\in\phi} S_i, S_i$ 是单模.

(b) S 是左 $R-$ 模 M 的单子模, T 是 M 的子模, 则要么 $S \bigcap T = \{0\}$, 要么 $S \subset T$.

定理 2.3.2 (单模的存在性). *任意环 R 上均有单模.*

证明. 证明过程当中需要使用 Zorn 引理, 证明的本质在于任意含幺环均有 (左) 极大理想. 令

$$T = \{I \mid I\text{为 } R \text{ 的左理想}, 1 \notin I\}$$

注意到, $T \neq \phi$, 至少 $0 \in T$, 考虑集合 T 上关于包含关系的偏序集 $(T, \subseteqq)$, 对于 T 中任意一条链:

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

由环的理想升链的封闭性: $1 \notin \bigcup\limits_{i=1}^{\infty} I_i \in T$. 即每条链都在集合 T 当中存在上界. 根据 Zorn 引理, 存在 T 中的极大元 I. 考虑左正则模 ${}_RR$, R_I 是左正则模的子模. 令 $M = R/I$, M 是左 $R-$ 正则模的商模. M 是单模, 否则, 根据模的对应定理, 存在 ${}_RR$ 的子模 $N \supseteq I$; 而左 $R-$ 正则模 ${}_RR$ 的子模与环 R 的左理想是一一对应的, 这与 I 的极大性矛盾. □

引理 2.3.3 (单模的等价刻画 1). *非零左 $R-$ 模 M 是单模, 当且仅当 $\forall 0 \neq x \in M, M = \langle x \rangle = Rx$.*

证明. ($\Rightarrow$): 设非零左 $R-$ 模 M 是单模, 任取 M 中的非零元 x; 考察 x 生成的子模: $\langle x \rangle = Rx$, 因为 M 是单模, 所以 $\langle x \rangle = Rx = M$.
($\Leftarrow$): 设 N 是 M 的非零子模, 则对于 $\forall x \in N$, $x \neq 0$, 且 $x \in M$, 由条件知 $\langle x \rangle = Rx = M \subseteqq M$, 从而 $M = N$, 即 M 无非平凡的子模, 即 M 是单模. □

引理 2.3.4 (循环模的等价刻画). *R 是一个环, 左 $R-$ 模 M 是循环模, 当且仅当存在左理想 I, 使得 $M \cong R/I$. 换句话说, 每一个左 R 循环模都同构于左 R 正则模 ${}_RR$ 的某个商模.*

证明. ($\Rightarrow$): 因为 M 是循环模, 故存在 $x \in M$ 使得, $M = \langle x \rangle = Rm$, 定义映射:

$$\begin{aligned} f :_R R &\mapsto_R M \\ r &\mapsto f(r) := rm \end{aligned}$$

容易验证 f为 $R-$ 同态, 并且注意到 f 是满同态. 由模同态第一定理, $\operatorname{Ker} f$ 是左正则模 R 的子模, 且 $R/\operatorname{Ker} f \cong M$. 同时, 由环 R 左正则模的子模与环 R 的左理想一一对应. $\operatorname{Ker} f$ 正是定理所需要的左理想.

($\Leftarrow$): 考虑环 R 上的左正则模 ${}_RR$, 左理想 I 对应左正则模 ${}_RR$ 的子模, 视 R/I 为左 R 正则模的商模, 其上生成元为 $1+I$, ${}_R(R/I) = \langle 1+I \rangle = \langle \overline{1} \rangle \cong M$, 即左 $R-$ 模 M 是循环模. □

注 19. 循环模的子模未必是有限生成的!

定理 2.3.5 (单模的等价刻画 2). *R 是一个环, 左 $R-$ 模 M 为是单模, 当且仅当存在极大左理想 I, 使得 $M \cong R/I$.*

证明. 根据单模的等价刻画 1, 单模是一类特殊的循环模 (它的每一个非零元素都可以是生成元); 根据循环模的等价刻画定理, 单模同构于左 R 正则模 ${}_RR$ 的某个商模. 根据模的对应定理, 环 R 左正则模的子模与环 R 的左理想一一对应, 而无非平凡子模对应于环 R 关于极大左理想 I 的左 $R-$ 商模 R/I, 即证. □

定理 2.3.6 (半单模的等价刻画). *R 是一个环, M 是左 $R-$ 模, 则以下等价:*
(1) M 是半单模
(2) $M = \sum\limits_{i \in I} S_i, S_i$ 是 M 的单子模. (若干单子模的和)
(3) $M = \bigoplus\limits_{i \in I} S_i, S_i$ 是 M 的单子模. (若干单子模的外直和)

(4) M 的每一个子模 $N \leqslant M$, 存在 M 的子模 $L \leqslant M$, 使得 $M = L \oplus N$.(每一个子模都是直和因子 (summand), 即存在直和补)

为了证明上述命题, 我们需要如下三个引理:

引理 2.3.7. *$M = \sum\limits_{\alpha\in I} M_\alpha$, I 是指标集, $M_\alpha \leqslant M$ 是单子模; 设 N 是 M 的子模, 则存在 $J \subset I$, 使得 $M = N \bigoplus (\bigoplus\limits_{J\subset I} M_\beta)$.*

注 20. 引理 2.2.7 是半单模等价刻画定理的弱形式. 引理 2.2.7 不但说明了一簇单子模的和等价于一簇单子模的直和; 而且说明了任意子模都是直和因子, 并且利用给的的单子模簇, 给出了直和补的具体形式. 一簇单模的和所构成的模是半单模, 其上任何子模都是直和因子.

证明. 设 N 为模 M 的任意子模, 令 $N := M_0$, 考虑指标集 I 的扩充 $S = I \bigcup \{0\}$. 下面, 我们首先采用 Zorn 引理说明若干单子模 $\{M_\alpha\}_{\alpha\in I}$ 的和模 M, 可以表示为任意给定的子模 N 与若干单子模的 $\{M_\alpha\}_{\alpha\in J}$ 直和, 其中 $J \in I$. 考虑关于指标集的集簇:

$$T = \{\Omega \subseteq S \mid 0 \in \Omega, \sum_{\alpha\in\Omega} M_\alpha = \bigoplus_{\alpha\in\Omega} M_\alpha\}$$

$T \neq \varnothing$, 至少 $\{0\} \in T$, 考虑集合 T 上的自然偏序 $(T, \subseteq)$. 设 T 中任意一条链:

$$\Omega_1 \subseteq \Omega_2 \subseteq \cdots \subseteq \Omega_n \subseteq \cdots$$

因为直和的支撑 (support) 具有有限性: 任取 $x \in \sum\limits_{\alpha\in\bigcup\limits_{i\geq 1}\Omega_i} M_\alpha$, 存在 $N \in \mathbb{N}$, 使得 $x \in \sum\limits_{\alpha\in\Omega_N} M_\alpha$. 根据链的定义, 因为元素表示法唯一, 所以我们有以下结论:

$$\sum_{\alpha\in\bigcup\limits_{i\geq 1}\Omega_i} M_\alpha = \bigoplus_{\alpha\in\bigcup\limits_{i\geq 1}\Omega_i} M_\alpha$$

于是, $\bigcup\limits_{i\geq 1}\Omega_i \in T$. 由 Zorn 引理, 集簇 T 中存在极大元 L. 令 $J = L - \{0\}$, 令 $M' := \sum\limits_{\alpha\in L} M_\alpha$, 于是根据 $L \in T$, $M' = N \bigoplus (\bigoplus\limits_{\beta\in J} M_\beta)$. 断言: $M' = M$. 否则, 如果 $M' \subsetneqq M$, 注意到单子模与子模的关系 (注释 12.(a)), 任何单子模 M_α 要么与子模 N 交为 $\{0\}$, 要么 $M_\alpha \in N$. 如果对于 $\forall\alpha \in I\backslash J$, $M_\alpha \in N$, 则 $M = M'$, 矛盾. 此时一定存在单子模 M_k,其中$k \in I\backslash J$, 使得 $M_k \bigcap N = \{0\}$. 此时 $M_k \bigcup M' = \{0\}$. 所以, $M + M_k = M \bigoplus M_k = \bigoplus\limits_{\alpha\in L\bigcap\{k\}} M_\alpha$, 这与 L 的极大性矛盾. □

引理 2.3.8. *如果非零模 M 的任意子模都有直和补, 则 M 有单子模.*

证明. 证明的关键在于: 单子模与子模的关系, 适当构造集合, 利用 Zorn 引理.
因为 $M \neq \{0\}$, 任取非零元素 $x \in M$, 借助非零元素 x, 考虑下面集簇:

$$T_x = \{N \mid N \leq M, x \notin N\}$$

$T_x \neq \varnothing$, 至少 $\{0\} \in T$. 考虑集合 T_x 上的自然偏序 $(T, \subseteq)$. 设 T_x 中任意一条链:

$$T_1 \subseteq T_2 \subseteq \cdots \subseteq T_n \subseteq \cdots$$

由模的链封闭性: $\bigcup\limits_{i\geq 1} T_i \in T$. 由 Zorn 引理, 集簇 T_x 中存在极大元 P. 因为 P 是 M 的子模, 由条件知存在直和补 $P' \leq M$, 使得 $M = P \bigoplus P'(P' \neq \{0\},)$ 否则矛盾. 现断言: P' 是模 M 的单子模. 否则, 存在 Q 为 P 的非平凡子模, 即 $Q \neq P'$, 且 $Q \neq \{0\}$. 根据直和补在同构的意义下是唯一的, 即 $P' \cong (P \bigoplus P')/P = M/P$. 根据模的对应定理, 商模 M/P 的子模与 P' 的子模是一一对应的. 即

$$\{H \mid H \leq P'\} \xleftrightarrow{\text{一一对应}} \{H' \mid P \subseteq H' \leq M\}$$

于是, 存在模 M 的子模 $M_1 \supseteq P$, 满足 $Q \cong M_1/P$. 由 P 的极大性, $x \in M_1$. 同样的, 因为 M_1 是模 M 的子模, 根据条件, 存在 $M_2 \leq M$, 使得 $M = M_1 \bigoplus M_2$. 模的直和分解具有可商性, 故 $P' \cong M/P = (M_1 \bigoplus M_2)/ = M_1/P \bigoplus M_2/P$. 注意到 $M_2/P \neq \{0\}$, 否则 $M_1 = M$, 这将导致 $Q = P'$(与 Q 的假设矛盾). 从而, 根据 P 的极大性, $x \in M_2$. 从而, $x \in M_1 \bigcap M_2 \neq \{0\}$, 这与 M_2 为 M_1 直和补矛盾. □

注 21. 实际上, 上述证明过程说明了: 非零子模 M 的任意子模存在直和补, 则对于任意非零元 $x \in M$, 包含元素 x 最小的子模就是单模, 即 x 生成的循环模 $\langle x \rangle$ 是单模. 这是单模等价刻画定理 1 局部化后的结果.

引理 2.3.9. *如果模 M 具有性质 P : 任何子模 $N \leqslant M$, N 在 M 中存在直和补; 则其子模和商模也具有性质 P.*

证明. 设 $N \leq M$ 是模 M 的子模, 对于子模 N 当中的任意子模 $L \leq N$, 注意到 L 也是 M 中的子模, 故由性质 P 得: 存在子模 L', 使得 $M = L \bigoplus L'$. 根据模的直和的自然继承性: $N = L \bigoplus (L' \bigcap N)$, 即子模满足性质 P. 对于模 M 的任意商模 M/N, 因为子模 N 具有性质 P, 故存在 $N' \leq M$, 使得 $M = N \bigoplus N'$. 直和补在同构的意义下是唯一的, 即 $M/N \cong N'$, N' 是模 M 的子模, 具有性质 P; 根据同构, 商模 M/N 具有性质 P. □

下面, 我们给出半单模等价刻画定理的证明:

证明. (i) (1) $\Longleftrightarrow$ (2) : 根据定义, 可得.

(ii) (2) $\Longrightarrow$ (3):
根据引理 2.2.7, 令 $N = \{0\}$ 即可.

(iii) (3) $\Longrightarrow$ (4): 根据引理 2.2.7, 即得.

(iv) (4) $\Longrightarrow$ (2): 根据引理 2.2.8, 对于 $\forall N \leq M$, N 均有直和补, 知 M 存在单子模. 令

$$M' = \sum_{\alpha \in I} M_\alpha; \quad \text{其中, 记集合} T := \{M_\alpha : M\text{的单子模}, I\text{是指标集}\}.$$

断言: $M = M'$; 否则: 如果 $M' \subsetneqq M$, 注意到子模的和仍为子模 (见模论第三节 $S + T = \langle S \bigcup T \rangle$), M' 是模 M 的子模. 根据 (4), 存在 $M'' \leq M$, 使得 $M = M' \bigoplus M''$. 根据引理 2.2.9, M'' 作为 M 的子模也满足性质 P, 故由 (4) 知存在单子模 $S \leqslant M'' \subsetneqq M$. 同样的, $S \leqslant M$, 即 $S \in T$. 从而 $\{0\} \neq S \subseteq M' \bigcap M'' \neq \{0\}$, 与直和补定义矛盾.

注 22. 事实上, 以上证明了对于半单模 M 可以完全分解为其上所有单子模的直和.

□

推论 2.3.10 (半单模的遗传性和可商性). *R 是一个环, 左 $R-$ 模 M 是半单模, 则 M 的每个子模, 商模也是半单模.*

证明. 根据引理(2.3.9), 半单模等价于任意非零子模具有性质 P, 性质 P 具有遗传性和可商性, 从而半单性具有可遗传性和可商性. □

2.3.2 半单环

定义 2.3.11. R 是一个环, 称 R 是一个**左半单环**, 若 R 是极小左理想的直和, 即 $R = \bigoplus\limits_{i \in I} I_i$, I_i 是 R 的极小左理想。

事实 1. 如果一个环 R 可以写成左理想的直和, 即 $R = \bigoplus\limits_{i \in I} L_i$, L_i 是 R 的左理想, 则仅有有限个左理想非零.

证明. $1 \in R = \bigoplus\limits_{i \in I} L_i$, 由外直和的支撑有限性, 不妨设:

$$1 = e_1 + e_2 + \cdots + e_n, e_i \in L_i$$

对于任意的 $a \in L_j$, 其中 $j \notin \{1, 2, \cdots, n\}$,

$$a = a \cdot 1 = ae_1 + ae_2 + \cdots + ae_n \in L_j \cap (L_1 \oplus L_2 \oplus \cdots \oplus L_n) = \{0\}$$

所以 $L_j = \{0\}$. 故 $R = L_1 \oplus L_2 \oplus \cdots \oplus L_n$. □

注 23. 一个环 R 是半单环, 那么它可以分解成有限个互不相交的极小左理想的直和.

推论 2.3.12 (半单环的有限可积性). $\{R_i\}_{i=1}^m$ 是 m 个半单环, 其中 $m \in \mathbb{N}$, 则它们的直积 $R = R_1 \times R_2 \times \cdots R_m$ 也是一个半单环.

证明. 因为 R_i 是半单环, 故存在极小左理想 $J_{i_{t(i)}}$, 使得:

$$R_i = J_{i_1} \bigoplus J_{i_2} \bigoplus \cdots \bigoplus J_{i_t(i)}$$

R_i 是环 R 的理想, 这只需要注意到 $R_i \cong \{(0, \cdots, 0, r_i, 0, \cdots, 0) \mid r_i \in R_i\}$. 更一般的, 任何有限直和 (积)$R_i$ 的左 (右) 理想都是 R 的左 (右) 理想 (容易验证). 有限外直和与有限外直积是同构的. 所以, 我们有以下分解:

$$R = \prod_{i=1}^{m} R_i \cong \bigoplus_{i=1}^{m} R_i = \bigoplus_{i=1}^{m} (\bigoplus_{j=1}^{t_{(j)}} J_{j_{t_{(j)}}})$$

□

下面我们看一些半单环的经典例子.

例 2.3.13 (除环的有限积是半单环). 除环 Δ 是单环, 也是半单环. $\{\Delta_i\}_{i=1}^m$ 是 m 个除环, 其中 $m \in \mathbb{N}$, 则它们的直积 $\Delta = \Delta_1 \times \Delta_2 \times \cdots \Delta_m$ 是一个半单环.

例 2.3.14 (域的有限积是可交换的半单环). 域 k 是单环, 其无非平凡的极小左立想, 但为半单环. $\{k_i\}_{i=1}^m$ 是 m 个域, 其中 $m \in \mathbb{N}$, 则它们的直积 $K = k_1 \times k_2 \times \cdots k_m$ 是一个可交换的半单环.

例 2.3.15. $\mathbb{Z}$ 是整数环, $p_1, p_2, \cdots, p_s$ 是 $\mathbb{Z}$ 中 s 个互不相同的素因子, $s \in \mathbb{N}$, 则 $n = p_1 p_2 \cdots p_s$ 是无平方因子数 (squarefree), $\mathbb{Z}_n$ 是一个半单环.

例 2.3.16. k 是一个域, $p_1(x), p_2(x), \cdots, p_s(x)$ 是域 k 中 s 个互不相同的不可约多项式, $s \in \mathbb{N}$, 则令 $f(x) = p_1(x)p_2(x) \cdots p_s(x)$, $k[x]/(f(x))$ 是一个半单环.

例 2.3.17 (主理想整环上的半单环构造). 更一般的, R 是一个主理想整环, $p_1, p_2, \cdots, p_s$ 是 R 中 s 个互不相同的不可约元 (素元), $s \in \mathbb{N}$, 记 $I_j = (p_j)$, 令 $n = p_1 p_2 \cdots p_s$. 根据中国剩余定理: R 是含幺环, $I_1, I_2, \cdots, I_s$ 两两互素, 对于主理想整环而言, $(n) + (m) = (\gcd(n, m))$,

$$R/(n) = R/(p_1 p_2 \cdots p_s = R/(I_1 \cap I_2 \cap \cdots I_s) \cong R/I_1 \bigoplus R/I_2 \bigoplus \cdots \bigoplus R/I_s$$

. 而对于任意的 $i \in \{1, 2, \cdots, s\}$, R/I_i 是域, 从而是半单环. 于是, $R/(n)$ 是半单环.

性质 2.3.18 (半单环上的模). R 是左半单环, 则每一个左 $R-$ 模 M 是半单模.

证明. 任何左 $R-$ 模 M 都是某个左 $R-$ 自由模的商模. 我们只需证明半单环上的自由模是半单模, 通过性质 P 的可商性, 即得. 设 F 为左 $R-$ 自由模, $\{x_i : i \in I, I$为指标集$\}$ 为 F 的基. 根据自由模定义, $F = \bigoplus\limits_{i\in I}\langle x_i\rangle \cong \bigoplus\limits_{i\in I} {}_RR$, 因为 R 为半单环, 所以左正则模 ${}_RR$ 为半单模, 从而 R_R 可以分解成单模的直和, 即 F 可以分解成单模的直和. 即, F 为半单模. 由性质 P 的可商性, 任何左 $R-$ 模 M 是半单模. □

性质 2.3.19 (左半单环的可商性). *R 为 (左) 半单环, I 是 R 的双边理想, 则 R/I 是 (左) 半单环.*

证明. 首先,R/I 是一个环. R 是半单环, 半单环上的模是半单模. 故,R/I 其作为左 $R-$模为半单模. 从而, 存在分解:

$$ {}_R(R/I) = \bigoplus_{j\in J} S_j, \quad \text{其中 } S_j \text{ 为 } R \text{ 上的单模.}$$

注意到, S_j 也是 R/I 上的单模 (S_j 被 I 零化, 从而有自然的数乘). 从而, R/I 上的左正则模为半单模, 即 R/I 为半单环.

□

注 24. 后面, Weddernburn–Artin 定理告诉我们: 每一个左半单环 R 都同构于除环上的全矩阵环的有限直积, 即

$$R \cong \mathrm{Mat}_{n_1}(\Delta_1) \times \mathrm{Mat}_{n_2}(\Delta_2) \times \cdots \times \mathrm{Mat}_{n_t}(\Delta_t)$$

其中, Δ_i 为除环, 并且除环 $\Delta_i (i = 1, 2, \cdots, t)$ 及整数 $t, n_1, n_2, \cdots, n_t$ 是环 R 的一组完全不变量.

Weddernburn–Artin 定理实际上给出了半单代数的分类; R 是半单环等价于左正则模 R 是半单模. 由此, 我们可以给出一些关于左半单环的分类结果:

(1) 一个交换环 R 是半单环, 当且仅当 $R = \bigoplus\limits_{i\in I}^{n} k_i \cong \prod\limits_{i=1}^{n} k_i$, 其中, 对于任意的 i, k_i 是域.

这是因为: 对于除环上的全矩阵环是交换环, 当且仅当 $n = 1, \Delta_i$ 是一个域.

(2) 以反环 (opposite Ring) 作为工具, 我们可得到: 每一个左半单环也是右半单环.

(3) 更一般的, 半单环既是左诺特环, 也是右诺特环.

2.3.3 Maschke 定理

下面, 我们介绍关于半单环最重要的一个例子, 它是表示论的开端.

定理 2.3.20 (Maschke 定理). *G 是一个有限群, k 是一个域, 则 $\mathrm{Char}\, k \nmid |G|$, 当且仅当群代数 kG 是一个左半单环.*

证明. 我们首先注意到半单环, 半单模, 半单代数, 直和补存在四者间的关系. 对于群代数 kG,

$$kG\text{为半单代数} \Leftrightarrow_{kG} kG\text{为半单模} \Leftrightarrow kG \text{ 半单环}$$

$$\Leftrightarrow \text{对于 } kG \text{ 的每个子模 (左理想)} I, \text{ 都存在直和补.}$$

$$\Leftrightarrow \text{对于 } kG \text{ 每个左理想 } I, \text{ 都存在收缩映射 } \rho : kG \mapsto I \text{ 为环同态}$$

$$\Longleftrightarrow \operatorname{Char} k \nmid |G|$$

下面, 我们证明: 对于 kG 的每个左理想 I, 收缩映射 ρ 的存在性 $\Longleftrightarrow \operatorname{Char} k \nmid |G|$.
kG 为域 k 上的向量空间, 设 I 为 kG 的任一左理想, 容易验证: I 是域 k 上向量空间 kG 的子空间. 由于线性空间的子空间总存在直和补, 于是存在子空间 V, 使得:

$$G = I \bigoplus V$$

对于任意 $u \in kG$, $u = b + v,\ b \in I,\ v \in V$ 表示法唯一. 考察子空间 I 上的自然投射:

$$d :\ kG \mapsto I$$

$$u \mapsto d(u) := b$$

d 是一个 $k-$ 线性变换, $\operatorname{Ker} d = V$; d 也是一个收缩映射, 但不是环同态. 下面, 我们利用线性空间上的收缩映射 d, 通过对 d 适当改造以得到群代数 kG 上的收缩映射. 对映射 d 采用平均处理 (averaging process), 构造群代数 kG 上的映射:

$$D : kG \mapsto kG$$

$$u \mapsto D(u) := \frac{1}{|G|} \sum_{x \in G} x d(x^{-1}u)$$

映射 D 是良定义的 $\Longleftrightarrow$ 在域 k 中, $|G| = |G| \cdot 1_k \neq 0 \Longleftrightarrow \operatorname{Char} k \nmid |G|$. 下面, 我们说明映射 D 为 kG 上的收缩映射, 且为环同态.

(a) $\operatorname{Im} D \subseteq I$: 若 $u \in kG, x \in G$, 则 $d(x^{-1}b) \in I$(投射 d 的定义). 因为 I 是左理想, $xd(x^{-1}b) \in I$, 于是 $D(u) \in I$.

(b) $D|_I = Id$, 即 $\forall b \in I$, $D(b) := b$: 任取 $b \in I$, $x_{-1}b \in I$, 于是 $d(x_{-1}b) = x_{-1}b$, 从而 $xd(x_{-1}b) = b$, 进而

$$\sum_{x \in G} x d(x^{-1}u) = |G| b$$

即

$$D(u) = \frac{1}{|G|} \sum_{x \in G} x d(x^{-1}u) = u$$

(c) D 是 kG 上的一个环同态: D 对 kG 上的加法保持运算可由 $k-$ 线性映射 d 保持加法运算直接得到. 这里仅需验证 D 对 kG 上的乘法保持运算, 而又根据 d 保持 k 上的数乘运算, 我们只需要验证:

$$\forall g \in G,\ u \in kG, D(gu) = gD(u)$$

通过计算

$$\begin{aligned} gD(u) &= \frac{1}{|G|}\sum_{x\in G} gxd(x^{-1}u) \\ &= \frac{1}{|G|}\sum_{x\in G} gxd(x^{-1}g^{-1}gu) \\ &= \frac{1}{|G|}\sum_{y=gx\in G} yd(y^{-1}gu) \\ &= D(gu) \end{aligned}$$

□

注 25. 关于上述定理, 我们有:

(1) $\mathrm{Char}\, k = 0$ 时, Maschke 定理也成立.

(2) A 是有限维代数, 称 A 为半单代数, 若 A 作为左正则模是半单模, 即 $A = \bigoplus_{i\in I} S_i, S_i$ 是单模. Maschke 定理还可以叙述为:k 是一个域, 有限群 G 的群代数 kG 是半单代数, 当且仅当 $\mathrm{Char}\, k \nmid \mid G \mid$.

(3) 当域 k 是代数封闭 (algebraically closed), Molien 定理(6.3.17)告诉我们如果

$$\mathrm{Char}\, k \nmid \mid G \mid$$

则群代数 kG 有:

$$kG \cong \mathrm{Mat}_{n_1}(k) \times \mathrm{Mat}_{n_2}(k) \times \cdots \times \mathrm{Mat}_{n_t}(k)$$

(4) 例如, 考虑复数域 $\mathbb{C}$ 上的半单群代数 $\mathbb{C}G$(半单性是因为 $\mathbb{C}$ 是特征为 0 的域, 根据 Maschke 定理, 群代数 $\mathbb{C}G$ 是半单代数), 因为复数域是代数封闭的, 故我们有:

$$\mathbb{C}G \cong \mathrm{Mat}_{n_1}(\mathbb{C}) \times \mathrm{Mat}_{n_2}(\mathbb{C}) \times \cdots \times \mathrm{Mat}_{n_t}(\mathbb{C})$$

其中, 我们可以证明以下结论 (半单群代数 $\mathbb{C}G$ 所包含有限群 G 的信息):

(a) $\dim(\mathbb{C}) = \mid G \mid$

(b) $\mid G \mid = n_1^2 + n_2^2 + \cdots + n_t^2$; (对同构式两边同取维数, 即得)

(c) 对于任意的 n_i, 我们有 $n_i \mid\mid G \mid$; (此性质的证明不是平凡的)

(d) 对于复数域 $\mathbb{C}$ 上的全矩阵环 $\mathrm{Mat}_n(\mathbb{C})$ 的个数 t, 实际上就是有限群 G 的共轭类.

(5) 存在有限群 G, H, 它们具有同构的复群代数 $\mathbb{C}H \cong \mathbb{C}G$, 但 $G \ncong H$.
例如, G, H 是两个有限交换群, 它们阶数均为 n; 作为复数域 $\mathbb{C}$ 上的群代数, 根据 Maschke 定理, $\mathbb{C}G$ 与 $\mathbb{C}H$ 是半单环; 根据 Wedderburn—Artin 定理, 半单环可以表示成有限个除环上全矩阵环的直积; 特别地, 对于可交换的半单环, 当且仅当可表示为有限个域的直积. 容易验证, 由于有限群 G, H 的可交换性质, 群代数 $\mathbb{C}G, \mathbb{C}H$ 是交换代数. 从而, 存在域 $\{k_i\}_{i=1}^m, m \in \mathbb{N}$, 使得:

$$\mathbb{C}G \cong k_1 \times k_2 \times \cdots k_m$$

因为复数域 $\mathbb{C}$ 是代数封闭的, 根据 Molien 定理, 对于任意的域 k_i, $k_i \cong \mathbb{C}$, 所以我们得到:

$$\mathbb{C}G \cong \mathbb{C} \times \mathbb{C} \times \cdots \mathbb{C} = \mathbb{C}^n$$

其中, $\mathbb{C}^n$ 是复数域的 n 维复射影空间.
综上所述, 阶数相同的有限交换群, 它们在复数域上的复群代数都是同构的! 更具体地, $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, 但作为有限交换群, 它们在复数域 $\mathbb{C}$ 上的复群代数是同构的. 我们很自然的会问: 在什么条件下, 我们可以从群代数的同构得到相应群的同构? 在单群的情况下, 上述问题是可以实现的, 这是得益于单群的分类已经完成, 我们可以对单群的群代数一一列举. 在代数学当中, 有一个与上述问题类似的 Huppert 猜想, 有兴趣者可阅读论文《Huppert's Conjecture for alternating groups》, Author: Christine Bessenrodt; Hung P. Tong-Viet; JiPing Zhang.

2.4 代数闭包

本节内容主要涉及:1. 代数闭包的存在唯一性; 代数闭包的直观; 代数整数环和代数数域部分小性质. 分别用超限归纳法和 Zorn 引理证明代数闭包的存在唯一性. 我们首先回顾一些关于域和域扩张的概念. 2. 介绍超限归纳法. Zorn 引理本质上是想扩大某个结构, 使得某些运算封闭; 而与之等价的良序公理实际上给了我们数学归纳法的推广(可以使运算封闭), 我将用 Zorn 引理和良序公理分别给出代数闭包存在唯一性的两种不同证明.

定义 2.4.1. k 是一个域, K/k 是一个域扩张, 称域 k 的扩域 K 是**代数扩域**, 若 $\forall a \in K$, a 为域 k 上的代数元, 即存在 $0 \neq f(x) \in k[x]$, 使得 $f(a) = 0$.

性质 2.4.2. *K/k 是一个域扩张, 对于代数元和域扩张, 我们有以下性质:*
(1) 若 $z \in K$, 则 z 是域 k 上的代数元, 当且仅当域扩张 $k(z)/k$ 为有限扩张.

(2) 若 $z_1, z_2, \cdots, z_n \in K$, 则 $z_1, z_2, \cdots, z_n$ 是域 k 上的代数元, 当且仅当域扩张 $k(z_1, z_2, \cdots, z_n)/k$ 为有限扩张.

(3) $y, z \in K$ 为域 k 上的代数元, 则 $y+z, y^{-1}, yz$ 都是域 k 上的代数元.

(4) 定义 $(K/k)_{alg} := \{z \in K \mid z$是域 k 的代数元$\}$, 则 $(K/k)_{alg}$ 是域 K 的一个子域.

证明. 参见 Rotman 英文原版书籍 *Advanced Algbra* Proposition B-2.36 Page. 339. □

定义 2.4.3. 给定一个域扩张 $\mathbb{C}/\mathbb{Q}$, 令

$$\begin{aligned}\mathbb{A} := (\mathbb{C}/\mathbb{Q})_{alg} &= \{z \in \mathbb{C} \mid z\text{为 } \mathbb{Q} \text{ 上的代数元}\} \\ &= \{z \in \mathbb{C} \mid \text{存在} 0 \neq f(x) \in \mathbb{Q}[x], \text{使得} f(z) = 0\}\end{aligned}$$

称 $\mathbb{A}$ 为**代数数域**, 代数数域的元素称为**代数数**.

类似的, 我们有代数整数, 可以证明: 任何代数数都可以表示成代数整数的商.

定义 2.4.4. 令

$$\mathbb{B} = \{z \in \mathbb{C} \mid \text{存在 } 0 \neq f(x) \in \mathbb{Q}[x], \text{使得} f(z) = 0\}$$

称 $\mathbb{B}$ 为**代数整数环**, 代数整数环的元素称为**代数整数**.

实际上, 代数数域和代数整数环有更一般的定义:

定义 2.4.5. 有理数域 $\mathbb{Q}$ 的有限次扩域 K 称为**代数数域** (有限扩域都是代数扩域, 即 K 中的元素都是代数元), 这是代数数论的基本研究对象, 一般简称数域. 如果扩张次数 $[K : \mathbb{Q}] = n$, 则称 K 为 n 次代数数域.

我们可以把有理数域 $\mathbb{Q}$ 的整数概念推广到任意代数数域上.

定义 2.4.6. 代数数 α 为**代数整数**, 若存在 $\mathbb{Z}[x]$ 上的首一多项式 $f(x)$, 使得 $f(\alpha) = 0$.

注 26. 我们列出代数数论当中的一些基本结果, 感兴趣的读者可参考代数数论的相关书籍.

(1) 因为域上的一元多项式是 PID, 故以下三个集合表示的意义相同:

$$\mathbb{A} = \{z \in \mathbb{C} \mid z\text{为 } \mathbb{Q} \text{ 上的代数元}\}$$

$$\{z \in \mathbb{C} \mid \text{存在} 0 \neq f(x) \in \mathbb{Q}[x], \text{使得} f(z) = 0\}$$

$$\{\alpha \in \mathbb{C} \mid \text{存在首一的不可约多项式 } \mathrm{Irr}(\alpha, \mathbb{Q}) \text{ 以 } \alpha \text{ 为根}\}$$

(2) 代数整数都是代数数.

(3) 整数 $\mathbb{Z}$ 都是代数整数; $\mathbb{Q}\backslash\mathbb{Z}$ 不是代数整数; Gauss 整数环 $Z[i]$ 是代数整数环

(4) 更一般地, 所有代数数构成的集合 $\mathbb{A}$ 叫做 $\mathbb{Q}$ 的代数闭包, 它是有理数域 $\mathbb{Q}$ 的无限次代数扩域. 每个数域 K 都是 $\mathbb{A}$ 的子域. 注意到, $\mathbb{A} \subsetneq \mathbb{C}$, 换句话说, 超越数是存在的, π 和e 是两个超越数. 除此之外, 我们指出超越数是严格比代数数多的; 这是因为代数数是可数的, 超越数不可数.

(5) 称代数数域 K 当中满足方程 $x^n - 1 = 0$ 的元素为 n **次单位根**; 特别地, 如果 n 次单位根的乘法阶数恰好就是方程的次数 n, 则称为 n **次本原单位根**. 代数数域 K 的单位根全体构成一个乘法群 U_K, 称为数域 K 的**单位根群**, 它是有限循环群. 任何 n 次单位根都是代数整数.

(6) 有理数域的代数闭包 $\mathbb{A}$ 是复数域 $\mathbb{C}$ 和有理数域 $\mathbb{Q}$ 的中间域, 但复数域 $\mathbb{C}$ 与 $\mathbb{R}$ 之间没有中间域.

性质 2.4.7 (域扩张塔 (tower) 的性质). *(1) 代数扩张具有**塔传递性**:$k \subseteq K \subseteq E$ 是一个域扩张塔, E/K与K/k 是代数扩张, 则 E/k 是代数扩张.*

*(2) 代数扩张具有**塔封闭性**:$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \cdots$ 是一个域扩张塔, 若 $\forall n \in \mathbb{N}$, K_{n+1}/K_n 为代数扩张, 则*

$$K = \bigcup_{n \geq 0} K_n$$

是域 K_0 的代数扩域.

(3) A 为一个集合, 令 $K = k(A)$, 若 $\forall a \in A$, a 是域 k 的代数元, 则 K/k 为代数扩张.

证明. 参见 Rotman 英文原版书籍 Advanced Algebra , Lemma B-2.38. Page. 340 . □

定义 2.4.8. 称域 K 是一个**代数封闭域** (Algebraically closed field), 若对于域 K 上的每个非常值多项式 $f(x) \in K[x]$, 存在 $a \in K$, 使得 $f(a) = 0$

定义 2.4.9. 称一个域 K 的代数扩域 $\bar{k}$ 为**代数闭包** (Algebra closure), 若代数扩域 $\bar{k}$ 是代数封闭的.

例 2.4.10. 下面, 我们给出一些代数闭包的重要例子.

(1) $\overline{\mathbb{Q}} = \mathbb{A} = \{z \in \mathbb{C} \mid z$为 $\mathbb{Q}$ 上的代数元$\}$; $\overline{\mathbb{R}} = \mathbb{C}$.

(2) 由代数基本定理知, 复数域 $\mathbb{C}$ 上的任何一元 n 次多项式 $f(x)(n \geq 1)$ 都至少有一个复数根. 换句话说, $\mathbb{C}$ 是一个代数闭域, 而有理数域 $\mathbb{Q}$ 的代数闭包 $\mathbb{A} \subsetneq \mathbb{R}$, 故 $\mathbb{C}/\mathbb{Q}$ 不是代数扩张.

注 27. 代数基本定理的证明, 最简单的是采用解析的办法: 复变函数中的 Liouville 定理和 Rouche 定理都可以实现. 纯代数的证明, 需要利用 Galois 理论将域 $\mathbb{C}$ 是代数封闭域这一问题转化为群论问题, 再结合 Sylow 定理计算 Galois 群的阶数为 2, 最后得出域扩张的次数为 1. 具体证明细节, 参见 Rotman 英文原版书籍 *Advanced Algbra* Page. 216.

下面, 我们给出关于代数闭包的两个重要结果:

(1) 代数闭包从直观上说是添加了域 k 上所有代数元形成的最大代数扩域.

(2) 每一个域 k 都存在代数闭包, 并且再同构的意义下是唯一的.

为了对上述结果分别用 Zorn 引理和超越归纳法证明, 展现两种方法在等价下的各自优劣, 我们先给出超越归纳法的相关概念, 算法和步骤. 对于超越归纳法, 在集合论的当中可以采用 "序数 (ordinal)" 给出有更严格的定义, 这里只给出我们通常使用的形式.

性质 2.4.11 (**超限归纳法** (transifinite induction))**.** *A 是一个良序集, $S_\alpha : \alpha \in A$ 为一簇命题语句. 如果以下两点成立:*

(a) 初始步骤 (Base Step): S_0 为真. (0 是良序集 A 的最小元)

(b) 演绎步骤 (Induction Step): 对于 $\forall r : 0 \leq r < \beta$, S_r 为真, 则可推出 S_β 为真.

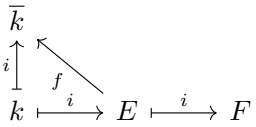
则我们对于 $\forall \alpha \in A$, 有 S_α 为真.

注 28. 一般情况下, 我们承认良序公理, 在对良序使用超限归纳法时, 只会涉及到良序的两类元素: 极限 (limit) 和后继 (successor). 称良序集 A 中元素 $y \in A$ 为**后继**, 若存在 $x \in A, x \leq y$并且$\forall z : x \leq z$, 我们有:$y \leq z$, 记为 $y = S(x)$. 称良序集 A 中元素 $y \in A$ 为**极限**, 若 $\forall x \in A, y \neq S(x)$. 特别地, 良序集中的极小元一定是极限.

定理 2.4.12 (**代数闭包的直观**)**.** *k 是一个域, $\overline{k}$ 为 k 的一个代数闭包, 若 F/k 是一个代数扩张, 则存在一个单同态 $\psi : F \mapsto \overline{k}$. 即任何一个代数扩张都可以嵌入到代数闭包.*

证明. 证明的基本思想: 延拓 (extension) 与逼近 (approximation). 借助 Zorn 引理实现逼近.

设 E 为一个中间域, $k \subseteq E \subseteq F$. 我们称有序对 (E, f) 为一个逼近 (approximation), 若 $f : E \mapsto \overline{k}$ 为 $k-$ 同态, 即 $f|_k = Id$. 此时, 有如下交换图:



定义: $X = \{(E, f) : \ k \subseteq E \subseteq F\}$. $X \neq \varnothing$. 因为至少 $(k, i) \in X$. 定义集 X 上的偏序:

$$(E, f) \preceq (E', f') \quad \text{当且仅当} \quad E \subseteq E', \ f'|_E = f$$

考虑偏序集 X 上的任意链 $S = \{(E_j, f_j) | j \in J, \text{ 其中 } J \text{ 为指标集}\}$, 我们断言

$$(\bigcup_{j \in J} E_j, \bigcup_{j \in J} f_j)$$

为链 S 的上界, 即 $(\bigcup\limits_{j\in J} E_j, \bigcup\limits_{j\in J} f_j) \in X$. 这是因为, 中间域的并仍是中间域 (事实). 下面, 我们说明 $\bigcup\limits_{j\in J} f_j$ 的含义: 令

$$\Phi = \bigcup_{j\in J} f_j : \bigcup_{j\in J} E_j \mapsto \overline{k}$$

$$u \in E_{j_0} \mapsto \Phi(u) := f_{j_0}(u)$$

Φ 是良定义的, 因为

$$E_{j_0} \subseteq E_{j_1},\ f_{j_1}|_{E_{j_0}} = f_{j_0}(\text{只需要注意到} f_{j_1} \text{延拓了} f_{j_0}).$$

同时 Φ 是一个 $k-$ 同态, 这是因为 $\forall j \in J$, f_j 是 $k-$ 同态, 而 Φ 恰好是通过链元素逐点定义的. 由 Zorn 引理, 存在 X 中的极大元 (E_0, f_0). 我们断言 $E_0 = F$. 若 $E_0 \subsetneqq F$, 则存在 $a \in F \setminus E_0$. 因为 F/k 是代数扩张, 所以 F/E_0 是代数扩张, 故存在 a 的极小多项式 $p(x) \in E_0[x]$, 使得 $p(a) = 0$(代数元的极小多项式一定存在, 这是因为域上多项式环是 PID).

单同态 $\quad f_0 : E_0 \mapsto \overline{k}$诱导了多项式环的同态

$$f_0^* : E_0[x] \mapsto \overline{k}[x]$$

$$\sum_{i=1}^{n} e_i x^i \mapsto \sum_{i=1}^{n} f(e_i) x^i$$

又因为 $\overline{k}$ 是代数封闭的, 故 $f_0^*(p(x))$ 在 $\overline{k}[x]$ 上有因子分解:

$$f_0^*(p(x)) = \prod_{i=1}^{n} (x - b_i), \quad \text{其中, } b_i \in \overline{k}$$

因为 $a \notin E_0$, 所以存在 b_i, 使得 $b_i \notin f_0(E_0)$, 于是我们定义:

$$f_1 : E_0(a) \mapsto \overline{k}$$

$$\sum_{j=1}^{n} c_j a^j \mapsto \sum_{j=1}^{n} f_0(c_j) b_i^j$$

其中, 注意到单代数扩张 $E(a) \cong E[a]$, 故 $\forall c_j,\ c_j \in E_0$. 映射 f_1 是良定义的. 容易验证 f_1 是一个 $k-$ 同态, 且 $f_1|_E = f_0$, $E \subseteq E(a)$ 是代数扩张. 于是, $(E(a), f_1)$ 与 (E_0, f_0) 的极大性矛盾. 即 $E_0 = F$, $\Psi = f_0 : E = F \mapsto \overline{k}$ 是单同态. □

下面证明当中, 我们需要借助一个**无限集上的多项式环**.

定义 2.4.13. 设 k 为一个域, T 是无限集, 称 $K[T]$ 为一个多项式环, 如果满足: 对于任意的 $t \in T$, 存在一个不定元. 即

$$K[T] = \bigcup_{U \subseteq T} k[U]$$

其中, U 是 T 的有限子集, $k[U]$ 和 k 上多元多项式环一一对应.

引理 2.4.14. *k 是一个域, $k[T]$ 是以集合 T 为不定元的多项式环, $t_1, t_2, \cdots, t_n \in T$ 是 n 个不同的元素 $(n \geq 2)$, 若 $f_i(t_i) \in k[t_i] \subseteq K[T]$ 为 n 个非常值多项式, 则 $I = (f_1(t_1), f_2(t_2), \cdots, f_n(t_n))$ 为非平凡理想.*

证明. (反证法) 假设 I 是平凡理想, 则 $1 \in I$, 于是存在 $h_i(T) \in k[T]$(整环 R 上的多元多项式环是 UFD):

$$1 = h_1(T)f(t_1) + \cdots + h_n(T)f(t_n)$$

考虑扩域 $k(\alpha_1, \alpha_2, \cdots, \alpha_n)$, 其中 α_i 是 $f_i(t_i)$ 的某个根. 记 $h_i(T)$ 中非 $t_1, t_2, \cdots, t_n$ 的不定元为 $t_{n+1}, \cdots, t_m$. 在扩域中赋值 $t_i = \alpha_i$ $(i \leq n)$, $t_i = 0$ $(i > n)$, 则等式左边为 1, 右边为 0, $0 = 1$, 矛盾. □

定理 2.4.15 (代数闭包的存在性). *k 是一个域, 存在 k 的代数闭包 $\overline{k}$.*

证明. (**方法一: 利用无限集多项式环和 Zorn 引理**)
考察集合 T 与下述集合对等:

$$\{p(x) \mid p(x) \text{ 为 } k[x] \text{ 上的非常值多项式}\}$$

构造多项式环 $R = k[T]$, 令 I 是所有由形如 $f(t_f)$ $(t_f \in T)$ 多项式生成的理想, 其中

$$f(t_f) = (t_f)^n + a_{n-1}(t_f)^{n-1} + \cdots + a_0, a_i \in k$$

断言: I 是非平凡理想. 否则, $1 \in I$, 存在 $t_1, t_2, \cdots, t_n \in T$ 和 $h_i(T) \in k[T]$, 使得

$$1 = h_1(T)f(t_1) + \cdots + h_n(T)f(t_n)$$

这与引理矛盾. 由 Zorn 引理, 存在包含 I 的极大理想 M, 于是 $K = R/M$ 为域. 我们称域 K 满足以下三点:

(a) K/k 为一个扩域.

首先, 我们有 $k \in K$, 这只需要注意到如下映射链:

令 $\theta = \pi \circ i : k \mapsto K$, 其中 π 是自然典范映射, i 是自然嵌入. θ 是单射, 这是因为任意域 k 到非零环同态是单射. 故 $\operatorname{Im}\theta \subseteq K$.

$$k \xrightarrow{\ i\ } R = K[T] \xrightarrow{\ \pi\ } K = R/M$$

图 2.1: 映射列

(b) $f(x) \in k[x]$ 为非常值多项式, 则 $f(x)$ 在扩域 K 上可分解. 对于每一个非常值多项式 $f(x) \in k[x]$, 都存在相应的 $t_f \in T$, 使得

$$f(t_f) = (t_f)^n + a_{n-1}(t_f)^{n-1} + \cdots + a_0 \in I \subseteq M$$

故 $f(t_f + M) = 0$, 其中 $t_f + M \in K$. $f(x)$ 在域 K 上可分解.

(c) K/k 为一个代数扩域. 这只需要注意到 $K = R/M \cong k(t_f + M)$, t_f遍历 T, $t_f + M$ 是域 k 上的代数元.

基于上述扩域 K, 我们构造一个代数扩张塔: 令 $K_1 = K$, 我们可以利用与非常值多项式对等的集合 T_n, 模仿上述 K 的构造过程, 从 K_n 构造 K_{n+1}. 从而我们得到: 代数扩域塔,

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \cdots \text{ 其中, } K_{n+1}/K_n \text{ 为代数扩域}$$

且 $K_n[x]$ 中每个非常值多项式 $f(x)$, 存在 $a \in K_{n+1}$, 使得 $f(a) = 0$. 令 $E = \bigcup\limits_{n\geq 0} K_n$ 为域 k 的代数扩域. 断言: E 是代数封闭的. 设 $g(x) = \sum\limits_{i=0}^{m} e_i x^i \in E[x]$ 为扩域 E 上的非常值多项式. 根据 E 的构造, 存在 $q \in \mathbb{N}$, 使得 $\{e_1, e_2, \cdots e_n\} \subseteq K_q$, 从而 $g(x) \in K_q[x]$. 则 $g(x)$ 在 $K_{q+1} \subseteq E$ 有根. 故 E 是代数封闭的. □

注 29. 上述定理证明中, 通过与域 k 上非常值多项式对等的集合, 赋值构造代数扩域 K. 事实上, 我们可以证明 K 是代数封闭的, 但证明是十分棘手的, 具体可参加 Isaacs. 为了减少困难, 我们构造代数扩张塔, 从更大的域出发证明代数封闭.

证明. (**方法二: 利用分裂域的存在性**)
$k[x]$ 是域 k 上的多项式环. 考虑集合,

$$S = \{p(x) \mid p(x) \text{ 为 } k[x] \text{ 上的不可约多项式}\}$$

遵循良序公理, 我们对 S 中的良序化. $(S, \prec)$ 是良序集. 下面, 我们借助不可约多项式的分裂域构造域扩张塔, 要求域扩张塔满足以下三条性质: 对于任意的 $p(x) \in S$, 满足:

(a) K_p 为 K 的代数扩张.

(b) $p(x)$ 在 K_p 内完全分解.

(c) 若 $q(x) \prec p(x)$, K_q 为 K_p 的子域.

我们采用超限归纳法进行构造: 设 $p_0(x)$ 为 S 中的极小元, 其在域 k 上的分裂域存在, 且在同构意义下唯一, 记为 K_{P_0}. 不妨设, 假设 $q(x) \prec p(x)$ 已构造出满足上述条件的代

数扩域

$$K_{q(x)} = \bigcup_{q_1(x) \preceq q(x)} K_{q_1(x)}$$

令

$$F = \bigcup_{q(x) \prec p(x)} K_q$$

代数扩张塔的封闭性, F 是代数扩张. 令 K_p 为 $p(x)$ 在 F 的分裂域. 即 K_p 满足 (1) ,(2) , (3). 令

$$\Omega = \bigcup_{p(x) \in S} K_p$$

Ω 是 k 的代数闭包.

注 30. 遵循良序公理, 通过给不可约多项式 $p(x)$"排序" 利用超限归纳法, 构造满足条件的域扩张塔. Rotman 英文原版书中给出了具体构造域扩张塔的方法, 而我们这里借助超限归纳法和分裂域, 避免了这个麻烦.

□

定理 2.4.16 (代数闭包的唯一性). *域 k 的任何两个代数闭包在同构的意义下是唯一的.*

证明. (**方法一: 利用代数闭包的直观**)
k 是域, K, L 为域 k 的两个代数闭包, 由代数闭包的直观定理. 存在 $K-$ 单同态和 $L-$ 单同态:

$$\Psi : K \mapsto L$$

$$\Theta : L \mapsto K$$

满足,

$$\Theta \circ \Psi = Id_K,\ \Psi \circ \Theta = Id_L$$

故 Ψ, Θ 为同构. 即 $L \cong K$. □

证明. (**方法二: 利用分裂域的唯一性**)
考虑集合,

$$S = \{p(x) \mid p(x) \text{ 为 } k[x] \text{ 上的不可约多项式}\}$$

遵循良序公理, 我们对 S 中的不可约多项式良序化. 设 $p_0(x)$ 为 S 中的极小元, 其在域 k 上的分裂域存在, 且在同构意义下唯一, 记为 K_{P_0}. 不妨设,

$$\forall p(x):\ p_0(x) \preceq p(x) \prec p_k(x),\ p(x) \text{ 的分裂域唯存在一, 记为 } K_p$$

则对于 $p_k(x)$, 其在 $F = \bigcup_{q(x)\prec p_k(x)} K_q$ 上的分裂域存在唯一. 根据超限归纳法, $\forall p(x) \in S$, 分裂域存在且唯一, 记为 K_P. 令

$$K = \bigcup_{p(x)\in S} K_p$$

根据代数闭包是最大的代数扩张, K 是代数闭包. 根据分裂域在同构下的唯一性, 它在同构下也是唯一的.

□

2.5 超越元与 Wedderburn 定理

介绍代数相关, 代数独立, 超越等定义, 并研究相关性质, 如: 验证超限归纳法合理性并借助其证明完全超越扩张的同构性质. 介绍独立, 生成, 基等概念, 引入超越基, 证明它的存在性, 并介绍超越基元素个数的性质. 证明韦德伯恩定理.

定理 2.5.1 (Wedderburn). *有限除环 D 是域; 即 D 中乘法为交换的.*

证明. 如果记 D 的中心为 Z, 则 Z 是有限域, 因此它有 q 个元素 (其中 q 是某个素数的幂). 由此 D 是 Z 上的向量空间, 从而有某个 $n \leq 1$ 使得 $\mid D \mid = q^n$; 即如果我们定义

$$[D : Z] = \dim_z(D)$$

则 $[D : Z] = n$. 如果能够证明 $n > 1$ 将导致矛盾, 即能完成证明.

如果 $a \in D$, 定义 $C(a) = \{u \in D : ua = au\}$. 容易证明 $C(a)$ 是包含 Z 的 D 的子除环. 由此, 有某个整数 $d(a)$ 使得 $\mid C(a) \mid = q^{d(a)}$, 即 $[C(a) : Z] = d(a)$. 我们不知道 $C(a)$ 是否可交换, 但已知

$$[D : Z] = [D : C(a)][C(a) : Z]$$

其中 $[D : C(a)]$ 表示 D 的作为 $C(a)$ 上的左向量空间的维数. 即 $n = [D : C(a)]d(a)$, 从而 $d(a)$ 是 n 的因数.

因 D 是除环, 它的非零元素 $D^\times$ 形成 $q^n - 1$ 阶乘法群. 群 $D^\times$ 的中心是 $Z^\times$, 并且如果 $a \in D^\times$, 则它的中心化子 $C_{D^\times}(a) = C(a)^\times$. 因此, $\mid Z(D^\times) \mid = q - 1$ 和 $\mid C_{D^\times}(a) \mid = q^{d(a)} - 1$, 其中 $d(a) \mid n$.

$D^\times$ 的类方程是

$$\mid D^\times \mid = \mid Z^\times \mid + \sum_i [D^\times : C_{D^\times}(a_i)]$$

其中从每个非中心的共轭类中选取一个 a_i, 但

$$[D^\times : C_{D^\times}(a_i)] = \mid D^\times \mid / \mid C_{D^\times}(a_i) \mid = (q^n - 1)/(q^{d(a_i)} - 1)$$

从而类方程变成

$$q^n - 1 = q - 1 + \sum_i \frac{q^n - 1}{q^{d(a_i)} - 1}$$

我们已经注意到每个 $d(a_i)$ 都是 n 的因数，而 a_i 不在中心的条件说明 $d(a_i) < n$.

回忆 n 阶分圆多项式是 $\phi_n = \prod(x - \xi)$, 其中 ξ 遍历一切 n 次单位原根. 我们已经证明对一切 i, $\phi_n(q)$ 是 $q^n - 1$ 和 $(q^n - 1)/(q^{d(a_i)} - 1)$ 的公因数, 因此上式给出

$$\phi_n(q) \mid (q - 1)$$

如果 $n > 1$ 且 ξ 是 n 次单位原根, 则 $\xi \neq 1$, 因此 ξ 是单位圆上的其他点. 因 q 是素数幂, 它是 x-轴上的一个点, 且 $q \geq 2$, 从而距离 $\mid q - \xi \mid > q - 1$. 所以

$$\mid \phi_n(q) \mid = \prod \mid q - \xi \mid > q - 1$$

矛盾, 由此可以知道, $n = 1$, 即 $D = Z$, 因此 D 是交换的. □

定义 2.5.2. 设 E/k 是域扩张. E 的子集 U 称为在 k 上**代数相关 (algebraically dependent)**, 如果存在有限子集 $\{u_1, \ldots, u_n\} \subseteq U$ 和非零多项式 $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ 使得 $f(u_1, \ldots, u_n) = 0$. 称 E 的子集 B **代数无关 (algebraically independent)**, 如果它不是代数相关的.

定义 2.5.3. 域扩张 E/k 称为**纯超越的 (pure transcendental)**, 如果不是 $E = k$ 就是 E 包含一个代数无关的子集 B 且 $E = k(B)$.

如果 $X = \{x_1, \ldots, x_n\}$ 是有限集, 则

$$k(X) = k(x_1, \ldots, x_n) = \mathrm{Frac}(k[x_1, \ldots, x_n])$$

叫做 n 个变量的函数域.

引理 2.5.4. *若 E/k 是纯超越扩张，且 $E = k(B)$, $B = \{u_1, \ldots, u_n\}$ 为有限代数无关的子集. 如果 $k(x_1, \ldots, x_n)$ 为以 $x_1, \ldots, x_n$ 为变量的函数域, 则存在一个同构 $\phi : k(x_1, \ldots, x_n) \to E$ 使得对任意 i 有 $\phi : x_i \mapsto u_i$.*

证明. 构造双射 $X = \{x_1, \ldots, x_n\} \to B$, 使得 $x_i \mapsto u_i$, 可扩充成同构

$$\phi : k[x_1, \ldots, x_n] \to k[u_1, \ldots, u_n]$$

再可扩充为分式域的同构

$$k(x_1, \ldots, x_n) \to k(u_1, \ldots, u_n)$$

□

注 31. 使用超限归纳法可以推广对 B 的有限性假设.

性质 2.5.5. *设 E/k 是域扩张, 并设 $U \subseteq E$, 则 U 在 k 上是代数相关的当且仅当存在 $u \in U$ 使得 u 是 $k(U-\{u\})$ 上的代数元素*

证明. 如果 U 在 k 上代数相关, 则存在代数相关的有限子集 $U' = \{u_1, \ldots, u_n\} \subseteq U$. 对 $n \geq 1$ 用数学归纳法证明有某个 u_i 是 $k(U' - \{u_i\})$ 上的代数元素. 如果 $n = 1$, 则存在某个非零多项式 $f(x) \in k[x]$ 使得 $f(u_1) = 0$, 即 u_1 是 k 上的代数元素. 而 $U' - \{u_1\} \neq \varnothing$, 所以 u_1 是 $k(U' - \{u_1\}) = k(\varnothing) = k$ 上的代数元素. 关于归纳步, 设 $U' = \{u_1, \ldots, u_{n+1}\}$ 代数相关的, 可以假定 $\{u_1, \ldots, u_n\}$ 是代数无关的. 因 U' 是代数相关的, 存在非零多项式 $f(X, y) \in k[x_1, \ldots, x_n, y]$ 使得 $f(\vec{u}, u_{n+1})$, 其中 $X = (x_1, \ldots, x_n)$, y 是新变量, $\vec{u} = (u_1, \ldots, u_n)$. 可以写 $f(X, y) = \sum_i g_i(X) y^i$, 其中 $g_i(X) \in k[X]$. 因 $f(X, y) \neq 0$, 有某个 $g_i(X) \neq 0$, 由此从 $\{u_1, \ldots, u_n\}$ 的代数无关性可知 $g_i(\vec{u}) \neq 0$. 所以 $h(y) = \sum_i g_i(X) y^i$ 不是零多项式. 但 $0 = f(\vec{u}, u_{n+1})$, 从而 u_{n+1} 是 $k(u_1, \ldots, u_n)$ 上的代数元素.

反之, 假定 u 是 $k(U - \{u\})$ 上的代数元素. 可以假定 $U - \{u\}$ 是有限的. 对 $n \geq 0$ 用数学归纳法证明 U 是代数相关的. 如果 $n = 0$ 则 u 是 k 上的代数元素, 因此 $\{u\}$ 是代数相关的. 关于归纳步, 设 $U - \{u_{n+1}\} = \{u_1, \ldots, u_n\}$. 可以假定 $U - \{u_{n+1}\} = \{u_1, \ldots, u_n\}$ 代数无关, 否则 $U - \{u_{n+1}\}$, 并因此它的超集 U 是代数相关的. 根据假设, 存在非零多项式 $f(y) = \sum_i c_i y^i \in k(u_1, \ldots, u_n)[y]$ 使得 $f(u_(n+1)) = 0$. 因 $f(y) \neq 0$, 可以假定它有一项, 比如 $c_j \neq 0$. 现在对每个 i, $c_i \in k(u_1, \ldots, u_n)$, 从而存在有理函数 $c_i(x_1, \ldots, x_n)$ 使得 $c_i(\vec{u}) = c_i$, 其中 $\vec{u} = (u_1, \ldots, u_n)$. 因 $f(u_{n+1})$, 我们可以通分, 从而可假定每个 $c_i(x_1, \ldots, x_n)$ 是 $k[x_1, \ldots, x_n]$ 中的多项式. 此外, $c_j(\vec{u}) \neq 0$ 蕴含 $c_j(x_1, \ldots, x_n) \neq 0$, 从而

$$g(x_1, \ldots, y) = \sum_i c_i(x_1, \ldots, x_n) y^i$$

非零. 所以 $\{u_1, \ldots, u_{n+1}\}$ 代数相关. □

定义 2.5.6. 集合 Ω 上的一个**相关关系 (relative relation)** 是指从 Ω 到 $\Phi(\Omega)$ 的关系 $\preceq$, 它满足下列公里:

1. 如果 $x \in S$, 则 $x \preceq S$;
2. 如果 $x \preceq S$, 则存在有限子集 $S' \subseteq S$ 使得 $x \preceq S'$;
3. (传递性) 如果 $x \preceq S$, 且有某个 $T \subseteq \Omega$ 满足对一切 $s \in S, s \preceq T$, 则 $x \preceq T$;
4. (交换公理) 如果 $x \preceq S$ 和 $x \npreceq S - \{y\}$, 则 $y \preceq (S - \{y\}) \cap \{u\}$.

引理 2.5.7. *如果 E/k 是域扩张, 定义 $a \preceq S$ 为 a 是 $k(S)$ 上的代数元素, 则 $a \preceq S$ 是一个相关关系.*

证明. 容易验证相关关系定义中的前两条公理, 现在我们验证公理 3: 如果 $x \preceq S$ 且有某个 $T \subseteq \Omega$ 满足对一切 $s \in S$ 有 $s \preceq T$, 则 $x \preceq T$. 如果 F 是一个中间域, 用 $\overline{F}$ 表示 F 上一切代数元素 $e \in E$ 组成的域. 使用这个记号, $x \preceq S$ 当且仅当 $x \in \overline{k(S)}$. 此外, 对一切 $s \in S$ 有 $s \preceq T$ 就是说 $S \subseteq \overline{k(T)}$, 由此, 根据引理, $x \in \overline{k(T)}$, 从而 $x \preceq T$.

交换公理说, 如果 $u \preceq S$ 且 $u \not\preceq S - \{v\}$, 则 $v \preceq (S - \{v\}) \cup \{u\}$. 记 $S' = S - \{v\}$, 于是 u 是 $k(S)$ 上的代数元素, 且 u 是 $k(S')$ 上的超越元素. 由于 $\{u, v\}$ 在 $k(S')$ 上是代数相关的, 从而存在非零多项式 $f(x, y) \in k(S')$ 使得 $f(u, v) = 0$. 更详细地说,

$$f(x, y) = g_0(x) + g_1(x)y + \cdots + g_n(x)y^n$$

其中 $g_n(x)$ 非零. 因 u 是 $k(S')$ 上的超越元素, 必有 $g_n(u) \neq 0$. 所以 $h(y) = f(u, y) \in k(S', u)[y]$ 是非零多项式. 但 $h(v) = f(u, v) = 0$, 因此 v 是 $k(S', u)$ 上的代数元素, 即:

$$v \preceq S' \cup \{u\} = (S - \{v\}) \cup \{u\}$$

□

定义 2.5.8. 设 $\preceq$ 是集合 Ω 上的相关关系. 子集 $S \subseteq \Omega$ 称为**相关的 (relative)**, 如果存在 $s \in S$ 使得 $s \preceq S - \{s\}$; 则称 S 是**无关的 (irrelevant)**, 如果它不是相关的. 我们说子集 S 生成 Ω 如果对一切 $x \in \Omega$ 有 $x \preceq S$. Ω 的一个基是指生成的无关子集.

在引理的相关关系下, 刚定义的无关与前面定义的代数无关是一致的.

引理 2.5.9. *设 $\preceq$ 是集合 Ω 上的相关关系. 如果 $T \subseteq \Omega$ 是无关的且有某个 $z \in \Omega$ 满足 $z \not\preceq T$, 则是 $T \cap \{z\} \not\supseteq T$ 严格较大的无关子集.*

证明. 因 $z \not\preceq T$, 公理 1 给出 $z \notin T$, 从而 $T \not\subseteq T \cup \{z\}$, 由此 $(T \cup \{z\}) - \{z\} = T$. 如果 $T \cup \{z\}$ 是相关的, 则存在 $t \in T \cup \{z\}$ 使得 $t \preceq (T \cup \{z\}) - \{t\}$. 如果 $t = z$, 则 $z \preceq T \cup \{z\} - \{z\} = T$, 和 $z \not\preceq T$ 矛盾. 所以 $t \in T$. 因 T 是无关的,$t \not\preceq T - \{t\}$. 如果在交换公理中令 $S = T \cup \{z\} - \{t\}$, $t = x$ 和 $y = z$, 则有:

$$z \preceq (T \cup \{z\} - \{t\}) - \{z\} \cup \{t\} = T$$

这和假设 $z \preceq T$ 矛盾, 所以 $T \cup \{z\}$ 无关. □

下面不加证明的推广交换引理.

定理 2.5.10 (交换引理的推广). *如果 $\preceq$ 是集合 Ω 上的相关关系, 则 Ω 有基. 事实上, Ω 的每个无关子集 B 都是一个基的一部分.*

定理 2.5.11 (**基的不变性**). 如果 Ω 是有相关关系 $\preceq$ 的集合, 则任意两个基 B 和 C 有相同的基数.

定义 2.5.12. 如果 E/k 是域扩张, 则一个**超越基 (transcendental basis)**B 是指 E 在 k 上的一个极大代数无关子集, E/k 的超越次数定义为

$$\mathrm{trdeg}(E/k) =\mid B \mid .$$

下一定理证明超越次数是合理定义的

定理 2.5.13 (**基的不变性**). 如果 E/k 是域扩张, 则存在超越基 B. 如果 $F = k(B)$, 则 F/k 是纯超越扩张且 E/F 是代数扩张. 此外, 如果 B 和 C 都是极大代数无关子集, 则 $\mid B \mid = \mid C \mid$.

2.6 Luroth 定理

本节主要介绍单超越扩张的结构以及相关性质. 首先, 回顾近世代数中域扩张的相关知识; 引入线性分式变换的概念并介绍其在单超越扩张中的性质; 证明吕洛特定理, 证明中需要用到本原多项式的相关知识.

定义 2.6.1. k 是一个域, 称 K 是域 k 的一个**扩域 (extension field)**, 若 $k \subset K$, 且 k 是 K 的子域. 记 K/k 是一个**域扩张 (extension)**. 称 K/k 是一个**有限扩张 (finite extension)**, 若 K 是域 k 上的有限维向量空间; 称 K 作为域 k 上的向量空间的维数为域扩张 K/k 的**次数 (degree)**, 记为 $[K : k]$. 称 K 作为域 k 上的向量空间的一组基为域扩张 K/k 的**基 (basis)**.

定义 2.6.2. K/k 是一个域扩张, 称 $a \in K$ 为域 k 上的**代数元 (algebraic element)**, 若存在非零多项式 $f(x) \in k[x]$, 使得 $f(a) = 0$. 否则称 a 为域 k 上的**超越元 (transcendence)**. 若对任意的 $a \in K$, a 是域 k 的代数元, 则称域扩张 K/k 为**代数扩张 (algebraic extension)**. 若存在 $\alpha \in K$, α 是域 k 上的超越元, 则称域扩张为**超越扩张 (transcendental extension)**.

定义 2.6.3. K/k 是一个域扩张, $\alpha \in K$, 称 $k(\alpha)$ 是域 k 上**添加元素** α 得到的扩域, $k(\alpha)$ 是包含 k 和 α 的一切子域的交. 更一般的, A 是 K 的子集, 称 $k(A)$ 是域 k 上**添加集** A 得到的扩域, $k(A)$ 是包含 k 和集 A 的一切子域的交. 若 $A = \{z_1, z_2, \cdots, z_n\}$, 可记扩域为 $k(z_1, z_2, \cdots, z_n)$.

定义 2.6.4. F 是一个域, 称 K/F 为**单扩张**, 若存在 $\alpha \in K$, 使得 $K = F(\alpha)$. 特别的, 若 α 为代数元 (超越元), 则称 K/F 为**单代数 (超越) 扩张 (simple algebraic/transcendental extensions)**.

定理 2.6.5 (有限扩张是代数扩张). *K/F 是有限扩张, 则对任意的 $\alpha \in K$, α 是域 F 上的代数元.*

证明. 设 $K/F = n$, 任取 $\beta \in K$, 则 $1, \beta, \cdots, \beta^n$ 在 F 上线性相关, 故存在不全为 0 的元素 $a_0, \cdots, a_n$, 使得 $a_0 + a_1\beta + \cdots + a_n\beta^n = 0$. 令

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$$

则

$$f(\beta) = 0, f(x) \neq 0$$

故 β 是 F 上代数元. □

定理 2.6.6 (单代数扩张是有限扩张). *K/F 是域扩张, $\alpha \in K$ 为 F 上的代数元, 设 α 在域 F 上的极小多项式 $\mathrm{Irr}(\alpha, F)$ 的次数为 n, 则 $[F(\alpha) : F] = n$, 且 $1, \alpha, \cdots, \alpha^{n-1}$ 为 $F(\alpha)$ 作为域 F 上的线性空间的一个基.*

证明. 设 $1, \alpha, \cdots, \alpha^{n-1}$ 在 F 上线性相关, 则有 F 中不全为 0 元素 $b_0, \cdots, b_{n-1}$, 使

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$$

令

$$g(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$$

则

$$g(\alpha) = 0, g(x) \neq 0$$

这与 α 在 F 上极小多项式次数为 n 矛盾, 故 $1, \alpha, \cdots, \alpha^{n-1}$ 线性无关, 而

$$F(\alpha) = F[\alpha] = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

故 $1, \alpha, \cdots, \alpha^{n-1}$ 是 $F(\alpha)$ 的一个基, 从而 $[F(\alpha) : F] = n$. □

注 32. 代数扩张不一定是有限扩张. 例如 $\mathbb{Q}$ 的代数闭包 $\mathbb{A}$.

注 33. 单超越扩张 $F(t)$ 同构于域 F 上一元多项式环 $F[x]$ 的分式域, 记为 $F(x)$.

定义 2.6.7. *k 是一个域, $k(x)$ 是域 k 上一元多项式环 $k[x]$ 的分式域. 对任意的 $\varphi \in k(x)$, 存在多项式 $g(x), h(x) \in k[x]$, 满足 $(g, h) = 1$, 使得 $\varphi = \frac{g(x)}{h(x)}$. 定义 φ 的次数为*

$$\deg(\varphi) = \max\{\deg(g(x)), \deg(h(x))\}$$

*称 φ 为域 k 上的**有理函数 (rational function)**, 称 $k(x)$ 为域 k 上的**有理函数域 (rational function fields)**.*

定义 2.6.8. k 是一个域, 称域 k 上的有理函数 φ 为**分式线性变换 (linear fractional transformation)**, 如果

$$\varphi = \frac{ax+b}{cx+d}$$

其中, $a,b,c,d \in k, ad-bc \neq 0$. 记域 k 上的全体分式线性变换的全体为 $\mathrm{LF}(k)$, 其中定义二元运算 (复合):

$$\varphi:\ x \mapsto \frac{ax+b}{cx+d}$$

$$\psi:\ x \mapsto \frac{rx+s}{tx+u}$$

$$\psi\circ\varphi:\ x \mapsto \frac{r\varphi(x)+s}{t\varphi(x)+u} = \frac{(ra+sc)x+(rb+sd)}{(ta+ud)x+tb+ud}$$

容易验证, $\mathrm{LF}(k)$ 关于上述复合运算构成一个群.

例 2.6.9. (1) $\deg(\varphi)=0$ 当且仅当 $\varphi \in k$

(2) $\deg(\varphi)=1$ 当且仅当 φ 为分式线性变换.

(3) 设 A 为域 k 上二阶一般线性变换群 $\mathrm{GL}(2,k)$ 的矩阵:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

我们有结论

$$\mathrm{LF}(k) = \frac{\mathrm{GL}(2,k)}{Z(2,k)}$$

其中, $Z(2,k)$ 是 $\mathrm{GL}(2,k)$ 的中心, $Z(2,k) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in k \right\}$.

证明. 考察映射

$$\zeta:\ \mathrm{GL}(2,k) \longrightarrow \mathrm{LF}(k)$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \frac{ax+b}{cx+d}$$

容易验证 ζ 是一个群同态, 且 $\operatorname{Ker}\zeta = Z(2,k)$ 于是 $\mathrm{PGL}(2,k) = GL(2,k)/Z(2,k) \cong LF(k)$. $PGL(2,k)$ 称为**一般射影线性群 (Projective General Linear)**. □

性质 2.6.10. 如果 $\varphi \in k(x)$ 不是常数, 则 φ 是 k 上的超越元素, 且 $k(x)/k(\varphi)$ 是有限扩张, 从而也是代数扩张, $[k(x):k(\varphi)] = \deg(\varphi)$.

证明. 设

$$g(x) = \sum a_i x^i$$
$$h(x) = \sum b_i x^i$$

则 $\theta(y) = g(y) - \varphi h(y)$ 是 $k(\varphi)[y]$ 中的多项式, 于是:

$$\theta(y) = \sum a_i y^i - \varphi \sum b_i y^i = \sum (a_i - \varphi b_i) y^i$$

如果 $\theta(y)$ 为 0 多项式, 则一切系数为 0. 设 b_i 为 $h(y)$ 的一个非零系数, 则由 $a_i - \varphi b_i = 0$, 得 $\varphi = \frac{a_i}{b_i}$ 为常数, 从而矛盾. 故 $\theta(y) \neq 0$,

$$\deg(\theta) = \deg(g(y) - \varphi h(y)) = \max\{\deg(g), \deg(h)\}$$

因 $\varphi = g(x)/h(x), x$ 为 $\theta(y)$ 的根, 故 x 是 $k(\varphi)$ 上的代数元素, $[k(x) : k(\varphi)]$ 有限. 设 φ 为 k 上代数元素, 则 $k(\varphi)/k$ 是有限的, 即 $k(\varphi) : k$ 有限, 从而

$$[k(x) : k] = [k(x) : k(\varphi)][k(\varphi) : k]$$

有限, 这与 x 是超越的矛盾, 故 φ 是 k 上超越元素. 我们断言 $\theta(y)$ 是 $k(\varphi)[y]$ 中不可约多项式. 如果 $\theta(y)$ 可约, 则 $\theta(y)$ 在 $k(\varphi)[y]$ 中可分解, 但 $\theta(y) = g(y) - \varphi h(y)$ 关于 φ 是线性的, 且 $h(x)$ 与 $g(x)$ 互素, 故 $\theta(y)$ 不可约, 且

$$[k(x) : k(\varphi)] = \deg(\mathrm{Irr}(x, k(\varphi))) = \deg(\theta) = \deg(\varphi).$$

□

推论 2.6.11. *$k(x)$ 为域 k 上的有理函数域, 设 $\varphi \in k(x)$, 则 $k(x) = k(\varphi)$, 当且仅当 φ 是分式线性变换.*

定义 2.6.12. *k 是一个域, E/k 是一个域扩张, 称同构 $\sigma : E \mapsto E$ 为 E 的 $k-$* **自同构**, *若 $\sigma|_k = Id$, 即对任意的 $a \in k$, $\sigma(a) = a$.*

定义 2.6.13. *E/k 是域扩张, 域 E 上的所有 $k-$ 自同构群关于映射的复合运算构成一个群, 称为域扩张 E/k 的* **Galois 群**, *记为 $\mathrm{Gal}(E/F)$.*

性质 2.6.14. *$k(x)$ 是域 k 上的有理函数域, 则 $\mathrm{Gal}(k(x)/k) \cong \mathrm{LF}(k)$.*

证明. 设

$$\sigma : k(x) \to k(x)$$
$$x \to x^\sigma$$

σ 为固定 k 的自同构, 因 σ 是满射, $k(x^\sigma)=k(x)$, 由第 67页推论 2.6.11, x^σ 是线性分式变换. 定义:

$$\gamma:\mathrm{Gal}(k(x)/k)\to \mathrm{LF}(k)$$
$$\gamma:\sigma\to x^\sigma$$

容易验证 γ 是同构. □

定理 2.6.15 (Luroth 定理). *k 是一个域, $k(x)/k$ 是一个单超越扩张, 则对于任意的中间域 B: $k\subseteq B\subseteq k(x)$, $B/k(x)$ 是一个单超越扩张. 即存在 $\varphi\in B\backslash k$, 使得 $B=k(\varphi)$.*

证明. 如果 $\beta\in B$ 不是常数, 则 $[k(x):k(\beta)]=[k(x):B][B:k(\beta)]$ 是有限的, 因此 $[k(x):B]$ 有限, 故 x 是 B 上的代数元素. 我们证明有 $\mathrm{Irr}(x,B)$ 的某个系数 φ 使 $B=k(\varphi)$. 设:

$$\mathrm{Irr}(x,B)=y^n+\beta_{n-1}y^{n-1}+\cdots+\beta_0\in B[y]$$

其中, $\beta_l\in B\subseteq k(x)$ 为有理函数. 设 $\beta_l=g_l(x)/h_l(x)$. 其中, $g_l(x),h_l(x)\in k[x]$, 且 $(g_l,h_l)=1$. 令 $f(x)=\mathrm{lcm}\{h_0,\cdots,h_{n-1}\}$, 所以对于任意的 l, 有 $u_l(x)\in k[x]$ 使得 $f(x)=u_l(x)h_l(x)$, 其最大公因式为 $\gcd\{u_0,\cdots,u_{n-1}\}=1$. 令:

$$i(x,y)=f(x)\,\mathrm{Irr}(x,B)=f(x)y^n+u_{n-1}g_{n-1}y^{n-1}+\cdots+u_0g_0\in k[x][y]$$

断言: $i(x,y)$ 为本原多项式. 如果 $i(x,y)$ 是非本原的, 则存在不可约多项式 $p(x)\in k[x]$, 整除 $f(x)$ 和每一个 u_lg_l, 对于每个 $l, f=u_lh_l$, 如果对每个 $l, p\nmid u_l$, 而 $p\mid f$, 则 $p\mid h_l$. 而 $(g_l,h_l)=1$, 故 $p\nmid g_l$. 但 $p\mid u_lg_l$, 所以 $p\mid u_l$, 矛盾. 所以对于所有 $l, p\mid u_l$, 而 $\gcd\{u_{n-1},\cdots,u_0\}=1$, 矛盾. 所以 $f(x)^{-1}$ 是 $\mathrm{Irr}(x,B)$ 的容度. 因 $i(x,y)$ 本原, 故 $i(x,y)=f(x)\,\mathrm{Irr}(x,B)$. 记出现在一个多项式 $a(x,y)$ 中 y 的最高指数为 $\deg_y(i)$, 则 $n=\deg_y(i)$. 设 $m=\deg_(\,xi)$, 注意到:

$$i(x,y)=f(x)y^n+\sum_{l=0}^{n-1}f(x)\beta_ly^l$$

则 $m=\max_l\{\deg(f),\deg(f\beta_l)\}$. 现在对一切 $l, h_l(x)\mid f(x)$, 从而 $\deg(h_l)\leqslant\deg(f)\leqslant m$, 而:

$$f\beta_l=(\mathrm{lcm}\{h_0,\cdots,h_{n-1}\}g_l)/h_l=(\mathrm{lcm}\{h_0,\cdots,h_{n-1}\}/h_l)g_l\in k[x]$$

所以 $\deg(g_l)\leqslant\deg(u_lg_l)=\deg(f\beta_l)\leqslant m$. 由此我们有 $\deg(g_l)\leqslant m$, 且 $\deg(h_l)\leqslant m$. $\mathrm{Irr}(x,B)$ 有某个系数 β_j 不为常数, 否则由定义 x 是 k 上的代数元素, 省略下标识, 记 $\beta_j=g(x)/h(x)$. 定义 $\varphi=\beta_j=g(x)/h(x)\in B$, 由第 66页性质 2.6.10, φ 是超越元素,

我们证明 $B = k(\varphi)$. 注意到 $g(y) - \varphi(h(y)) = g(y) - g(x)h(x)^{-1}h(y)$ 以 x 为根, 而 $\mathrm{Irr}(x, B)$ 在 $k(x)[y]$ 中整除 $g(y) - \varphi h(y)$, 故存在 $q(x, y) \in k(x)[y]$ 使得:

$$\mathrm{Irr}(x, B)q(x, y) = g(y) - \varphi h(y). \tag{2.1}$$

因为 $g(y)-\varphi h(y) = h(x)^{-1}(h(x)g(y)-g(x)h(y))$, 且 $(h(x), g(x)) = 1$, 所以容度 $c(g(y)-\varphi h(y))$ 为 $h(x)^{-1}$ 且其相伴本原多项式为:

$$\phi(x, y) = h(x)g(y) - g(x)h(y),$$

其中, $\phi(x, y) \in k[x][y]$, $\phi(y, x) = -\phi(x, y)$. 注意到, (2.1) 式可变形为:

$$f(x)^{-1}i(x, y)c(q)q(x, y)^*h(x) = \phi(x, y)$$

其中, $c(q) \in k(x)$ 是 $q(x, y)$ 的容度. 由 Gauss 引理, $i(x, y)q(x, y)^*$ 是本原的, 而 $\phi(x, y) \in k[x][y]$, 故 $f(x)^{-1}c(q)h(x) \in k[x]$. 定义 $q^{**}(x, y) = f(x)^{-1}c(q)h(x)q(x, y)^*$, 则 $q^{**}(x, y) \in k[x, y]$, 于是, $i(x, y)q^{**}(x, y) = \phi(x, y)$. 我们计算上式中的次数, 左端关于 x 的次数为:

$$\deg_x (iq^{**}) = \deg_x(i) + \deg_x(q^{**}) = m + \deg_x (q^{**})$$

而右端关于 x 的次数为:

$$\deg_x \phi = \max\{\deg g, \deg(h)\} \leqslant m$$

所以 $m + \deg_x q^{**} \leqslant m$, $\deg_x q^{**} = 0$, 即 $q^{**}(x, y)$ 是一个关于 y 的函数. 注意到 $\phi(x, y)$ 是 x 的本原多项式, 且 $\phi(y, x) = -\phi(x, y)$, 故其是关于 y 的本原多项式, 故其系数应在 $k[x]$ 中互素. 注意到 $\phi(x, y) = i(x, y)q^{**}(x, y)$. $i(x, y)$ 是本原的, 所以 q^{**} 只能是一个常数, $i(x, y)$ 和 $\phi(x, y)$ 在 $k[x, y]$ 中相伴, 所以:

$$\deg_x(\phi) = \deg_x(i) = m$$

$$m = \deg_x(\phi) = \max\{\deg(g), \deg(h)\}$$

由 ϕ 的对称性知, $\deg_y(\phi) = \deg_x(\phi)$, 所以:

$$n = \deg_y(\phi) = \deg_x(\phi) = m = \max\{\deg(g), \deg(h)\}$$

而 $\deg(\phi) = \max\{\deg(g), \deg(h)\} = m$. 由第 66页性质 2.6.10, $[k(x) : k(\phi)] = m$, 由 $\phi \in B$, 我们有:

$$[k(x) : k(\phi)] = [k(x) : B][B : k(\phi)]$$

而 $[k(x) : B] = n = m$, 故 $[B : k(\phi)] = 1$, 即 $B = k(\phi)$. □

第三章　模的范畴

3.1　范畴

本次内容主要介绍范畴的概念, 范畴是一个更加普适的语言, 在范畴中我们可以发现群、环、模并不是独立的体系. 它们都可以用范畴的语言表示. 当然, 包括一些子范畴, 反范畴, 离散范畴, 积与余积等概念和一些简单命题的证明.

定义 3.1.1. 一个**范畴 (category)**$\mathcal{C}$ 由三要素组成: **类 (class)** 的**对象 (object)**$\mathrm{obj}(\mathcal{C})$; 对每个有序对象对 (A,B) 的**态射 (morphism)**$\mathrm{Hom}(A,B)$ 集合; 对每个有序三对象组 (A,B,C) 的**复合 (composition)**:

$$\begin{aligned}\mathrm{Hom}(A,B)\times Hom(B,C)&\mapsto Hom(A,C)\\(f,g)&\mapsto gf\end{aligned}$$

这三个要素受到下面三个公理的限制:

(1) Hom 集合是两两**不相交的 (disjoint)**, 即每个态射由唯一的定义域和目标域.

(2) 对每个对象 A, 有一个**单位态射 (identity)**$1_A\in\mathrm{Hom}(A,A)$ 满足对一切:$f:A\to B$ 有:

$$f\circ 1_A=f;1_B\circ f=f$$

(3) 复合是**结合的 (associative)**: 给定态射: $A\xrightarrow{f}B\xrightarrow{g}C\xrightarrow{h}D$

$$h\circ(g\circ f)=(h\circ g)\circ f$$

例 3.1.2. 下面给出一些范畴的例子.

(1) 实向量空间构成的范畴. 类: 所有实向量空间; 态射: 线性变换; 复合: 线性变换复合.

(2) 群范畴. 对象: 所有的群; 态射: 群同态; 复合: 普通的复合.

(3) 交换环范畴. 对象: 所有的交换环; 态射: 环同态; 复合: 普通的复合.

(4) ${}_R\mathrm{Mod}$ 范畴. R 是一个环. 范畴的对象是 $R-$ 模; 态射是 $R-$ 模同态; 复合是通常映射的复合; 我们记 ${}_R\mathrm{Mod}$ 中的 $\mathrm{Hom}(A,B)$ 为:

$$\mathrm{Hom}_R(A,B)$$

如果 $R=\mathbb{Z}$, 我们常写

$${}_{\mathbb{Z}}\mathrm{Mod}=\mathrm{Ab}$$

即 $\mathbb{Z}-$ 模就是 Abel 群.

(5) 偏序集范畴 $\mathcal{C}=PO(X)$. 其中 X 是偏序集, 把它看作一个范畴, 其对象是 X 的元素, Hom 集或者是空集或者只有一个元素:

$$\mathrm{Hom}(x,y)=\begin{cases}\varnothing & x\not\preceq y\\ \{k_y^x\} & x\preceq y\end{cases}$$

其中, 符号 k_y^x 表示 $x\preceq y$ 时在 Hom 集中的唯一的元素. 复合由以下规则给出:

$$k_z^y k_y^x=k_z^x$$

注意由自反性, $1_A=k_x^x$. 因偏序关系是传递的, 所以复合有意义.

(6) $\mathcal{C}=\mathcal{C}(G)$. 其中 G 是一个群, 则下面的描述定义范畴 $\mathcal{C}(G)$: 它只有一个对象 $*$, 它的态射集为:

$$\mathrm{Hom}(*,*)=G$$

复合即 $G\times G\to G$ 是 G 中给定的乘法.

定义 3.1.3. 范畴 $\mathcal{C}$ 称为**离散的 (discrete)**, 若对于 $\mathcal{C}$ 中的任意对象 $x,y\in\mathcal{C}$ 有:

$$\mathrm{Hom}_{\mathcal{C}}(x,y)=\begin{cases}\{Id_x\} & x=y\\ \varnothing & x\neq y\end{cases}$$

定义 3.1.4. 范畴 $\mathcal{D}$ 称为范畴 $\mathcal{C}$ 的**子范畴 (subcategory)**. 若 $\mathrm{obj}(\mathcal{D})$ 是 $\mathrm{obj}(\mathcal{C})$ 的子类, 并且对 $\mathcal{D}$ 的任意对象 x,y:

$$\mathrm{Hom}_{\mathcal{D}}(x,y)\subseteq\mathrm{Hom}_{\mathcal{C}}(x,y)$$

同时, 对于 $\mathcal{D}$ 中的对象 x,x 在 $\mathcal{D}$ 中的恒等态射跟在 $\mathcal{C}$ 中的恒等态射相同. $\mathcal{D}$ 中的态射的合成跟在 $\mathcal{C}$ 中的合成法则相同.

定义 3.1.5. 范畴 $\mathcal{C}$ 的**反范畴 (opposite category)**$\mathcal{C}^{op}$ 的对象就是 $\mathcal{C}$ 中的对象, 态射集为:

$$\mathrm{Hom}_{\mathcal{C}^{op}}(x,y)=\mathrm{Hom}_{\mathcal{C}}(y,x)$$

一个显然的事实是 $(\mathcal{C}^{op})^{op}=\mathcal{C}$.

定义 3.1.6. 范畴 $\mathcal{C}$ 与范畴 $\mathcal{D}$ 的**积范畴 (product category)**$\mathcal{C}\times\mathcal{D}$ 的对象为二元组 (C,D), 其中 $C\in\mathcal{C}, D\in\mathcal{D}$. 态射集定义为:

$$\mathrm{Hom}_{C\times D}((C,D),(C',D'))=\mathrm{Hom}_{\mathcal{C}}(C,C')\times\mathrm{Hom}_{\mathcal{D}}(D,D')$$

态射的复合为各个分量的复合.

定义 3.1.7. 范畴 $\mathcal{C}$ 中的态射 $f:X\to Y$ 为**单态射 (monomorphism)**, 若对满足 $fg=fh$ 的任意态射 $g,h\in\mathrm{Hom}_{\mathcal{C}}(Z,X)$, 必有 $g=h$, 记为 $X\hookrightarrow Y$. 对偶的, 态射 $f:X\to Y$ 称为**满态射 (epimorhism)**, 如果对于满足 $gf=hf$ 的任意态射 $g,h\in\mathrm{Hom}_{\mathcal{C}}(Y,Z)$, 必有 $g=h$, 记为 $X\twoheadrightarrow Y$.

定义 3.1.8. 称范畴 $\mathcal{C}$ 中的态射 $f:A\to B$ 为**同构 (isomorphsim)**, 如果存在 $\mathcal{C}$ 中的态射 $g:B\to A$ 使得:

$$g\circ f=1_A \text{ 和 } f\circ g=1_B.$$

称态射 g 为 f 的**逆 (inverse)**, 且逆是唯一的.

定义 3.1.9. 称范畴 $\mathcal{C}$ 具有**预加性 (pre-additive)**, 如果每个 $\mathrm{Hom}(A,B)$ 配置有二元加法运算使它变成一个 Abel 群, 且对于这个运算分配律成立: 对一切 $f,g\in\mathrm{Hom}(A,B)$,

(1) 如果 $p:B\to B'$, 则 $p\circ(f+g)=p\circ f+p\circ g\in\mathrm{Hom}(A,B')$;

(2) 如果 $q:A'\to A$, 则 $(f+g)\circ q=f\circ q+g\circ q\in\mathrm{Hom}(A',B)$.

定义 3.1.10. 范畴中的一个**图 (graph)** 是指**有向多重图 (multi-directional graph)**, 它的**顶点 (vertical)** 是 $\mathcal{C}$ 中的对象, 它的**箭头 (arrow)** 是 $\mathcal{C}$ 中的态射.

例如: $\begin{array}{ccc} X & & \\ \downarrow{\scriptstyle f} & \searrow{\scriptstyle h} & \\ Y & \xrightarrow{g} & Z \end{array}$ $\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle g'} & & \downarrow{\scriptstyle g} \\ C & \xrightarrow{f'} & D \end{array}$ 都是交换图.

定义 3.1.11. 称**图交换 (commutative)**, 如果对每个顶点 A 和 B, 从 A 到 B 的任意两条路径相等, 即复合是相同的态射.

例如, 如果 $g\circ f=h$, $k\circ f=h$ 则上面的图交换.

我们可以" 分离" 两个集合使其没有重叠的部分. 考虑笛卡尔积

$$(A\cup B)\times\{1,2\}$$

并考虑子集 $A'=A\times\{1\}$ 和 $B'=B\times\{2\}$. 显然 $A'\cap B'=\varnothing$, 因为:

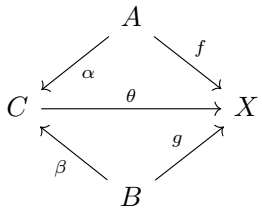
$$(a,1)\neq(b,2); a\in A, b\in B$$

称 $A' \cup B'$ 为 A 和 B 的不相交并. 注意由 $\alpha : a \mapsto (a, 1)$ 和 $\beta : b \mapsto (b, 2)$ 给出的函数 $\alpha : A \to A'$ 和 $B \to B'$. 记不相交并 $A' \cup B'$ 为 $A \sqcup B$. 如果对于某个集合 X 有函数 $f : A \to X$ 和 $g : B \to X$, 则存在唯一的函数 $h : A \cup B \to X$, 它由如下关系给出:

$$h(u) = \begin{cases} f(u) & u \in A \\ g(u) & u \in B \end{cases}$$

因为 A, B 是不相交的, 所以定义有意义. 下面我们用范畴来描述这个构造.

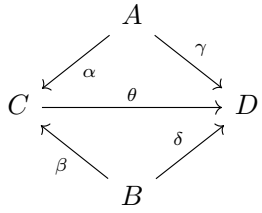
定义 3.1.12. 如果 A, B 是范畴 $\mathcal{C}$ 中的对象, 则它们的**余积 (coproduct)** 是指 $\mathrm{obj}(\mathcal{C})$ 中的一个对象 $\mathcal{C}$ 连同**内射态射 (injection)**$\alpha : A \to A \sqcup B$ 和 $\beta : B \to A \sqcup B$ 满足对 $\mathcal{C}$ 中每个对象 X 和每对态射 $f : A \to X$, $g : B \to X$, 存在唯一的态射 $\theta : A \sqcup B \to X$ 使得下图交换. 记 A 和 B 的余积为 $C = A \sqcup B$.



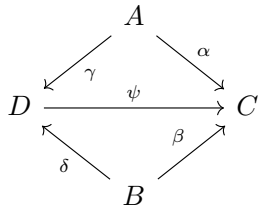
对上述构造的集合 $A \sqcup B = A' \cup B' \subseteq (A \cup B) \times \{1, 2\}$, 容易验证其是集合范畴中的余积.

性质 3.1.13. *如果 $\mathcal{C}$ 是范畴, A, B 是 $\mathcal{C}$ 中的对象, 如果 A, B 的任意两个余积存在, 则在同构意义下是唯一的.*

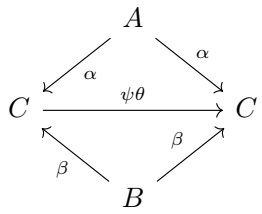
证明. 假设 C, D 是 A, B 的两个余积. 更详细的说, 假定 $\alpha : A \to C, \beta : B \to C, \gamma : A \to D, \delta : B \to D$ 是内射态射. 如果在定义 C 的图中取 $X = D$, 则存在态射 $\theta : C \to D$ 使下图交换:



同样, 在 D 的图中, 取 $X = C$, 我们得到态射 $\psi : D \to C$ 使下图交换:

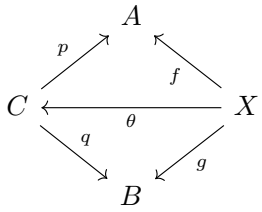


考虑下面两个图, 它是由上面两个图拼接起来的:



因为 $\psi\theta\alpha = \psi\gamma = \alpha$, $\psi\theta\beta = \psi\delta = \beta$, 所以这个图交换. 显然 $1_C : C \to C$ 也使得图交换. 又有 $C \to D$ 的唯一性, 则 $C \to C$ 是唯一的, 所以 $1_C = \psi\theta$. 同样可以论证 $\theta\psi = 1_D$. 由此 $C \to D$ 是同构的. □

定义 3.1.14. 如果 A, B 是范畴 $\mathcal{C}$ 中的对象, 则它们的**积 (product)**, 记作 $A \sqcap B$, 指 $\mathrm{obj}(\mathcal{C})$ 中的一个对象 $\mathcal{P}$ 连同**态射** $p : P \to A$ 和 $q : P \to B$ 满足对 $\mathcal{C}$ 中每个对象 X 和每对态射 $f : X \to A, X \to B$, 存在唯一的态射 $\theta : X \to P$ 使得下图交换.



两个集合 A 和 B 的的范畴积为 $P = A \times B$ 是集合中的笛卡尔积. 定义 $p : A \times B \to A$ 为 $p : (a, b) \mapsto a; q : (a, b) \mapsto b$. 如果 X 是集合, 则 $f : X \to A; g : X \to B$ 是函数, 可以证明由 $\theta : x \mapsto (f(x), g(x)) \in A \times B$ 定义的 $\theta : X \to A \times B$ 满足必需条件.

性质 3.1.15. *如果 A, B 是范畴 $\mathcal{C}$ 中的对象, 则 A 和 B 的积在同构意义下是唯一的.*

证明. 此证明参考余积在同构意义下唯一性的证明, 它们是对偶的. □

3.2 函子

学习有关函子的一些基本性质, 介绍了双边模的定义, 性质及 Hom 函子.

定义 3.2.1 (协变函子 (covariant functor)). 设 $\mathcal{C}, \mathcal{D}$ 为两个范畴, 在范畴之上构造映射 T, 使得满足下列条件:

(1) 对于 $\mathcal{C}$ 中的对象 $A \in \mathrm{obj}(\mathcal{C})$, $T(A) \in \mathrm{obj}(\mathcal{D})$

(2) 对于态射 $f : A \to B$, 给出 $T(f) : T(A) \to T(B)$.

(3) (结合律) 对于态射 $A \xrightarrow{f} A' \xrightarrow{g} A''$, 我们有 $T(A) \xrightarrow{T(f)} T(A') \xrightarrow{T(g)} T(A'')$ 满足:

$$T(gh) = T(g)T(h)$$

(4) (恒等态射) 对任意的 $A \in \mathrm{obj}(C), T(1_A) = 1_{T(A)}$.

对比范畴的定义 (范畴构成的要素是对象, 对象之间的态射, 态射要满足结合性质, 恒等态射存在), 我们可以知道函子的定义是十分合理的. 从另个角度看, 如果把一个范畴看作对象, 那么函子就是范畴之间的态射 (范畴的范畴).

一种比较重要的函子是由模范畴到 Abel 群畴的 $\mathrm{Hom}(M, *)$ 函子:

定义 3.2.2 (Hom(A,*) 函子). 考虑任意的范畴 $\mathcal{C}$, 函子:

$$\begin{aligned} T_A : \mathcal{C} &\to \mathrm{Sets} \\ X &\to \mathrm{Hom}(M, X) \end{aligned}$$

其中, 态射 $f : B \to B'$ 对应 $T(f) : h \mapsto fh, h \in \mathrm{Hom}(A, B), fh \in \mathrm{Hom}(A, B')$. 上述的态射 $T(f)$ 可以记成 f_*, 是为诱导出来的一种映射. 出于简便, 记 T_A 为 $\mathrm{Hom}(A, *)$.

可以验证上面的定义关于结合性是成立的:

$$T(fg) : h \mapsto gh \mapsto f(gh)$$

$$T(f)T(g) : h \mapsto g_*h = gh \mapsto f_*(gh) = f(gh)$$

恒等态射满足 $(1_A)_* : h \mapsto 1_A h = h$.

上述函子是从模范畴到 Abel 群范畴上的函子, 它的重要性在于保持了正合列, 这是同调代数的基本实例.

定理 3.2.3 ($\mathrm{Hom}(A, *)$ **函子的左正合性**). *若有 $R-$ 模构成的正和列:*

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C$$

上述正合列在 $\mathrm{Hom}(X, *)$ 函子作用下保持左正合性:

$$0 \to \mathrm{Hom}(X, A) \xrightarrow{i_*} \mathrm{Hom}(X, B) \xrightarrow{p_*} \mathrm{Hom}(X, C)$$

上述序列是正合列, 它是左正合的.

证明. 首先计算 $\mathrm{Ker}(i_*)$, 设 $f \in \mathrm{Ker}(i_*)$, $i_*(f) = i(f) = 0$. 考虑到 i 的单射性, 给出 $if(x) = 0, f(x) = 0, f = 0$. 其次, 由 $p_*i_*f = (pi)f = 0f = 0$ 得知 $\mathrm{Im}(i_*) \subseteq \ker(p_*)$. 最后考虑 $f \in \mathrm{Ker}(p_*)$, 我们有 $p_*(f) = pf = 0$ 给出任意的 $x \in X, f(x) \in \mathrm{Ker}(p)$, 由正合列的正合性, 即 $\mathrm{Ker}(p) = \mathrm{Im}(i)$ 给出存在 $a \in A, i(a) = f(x)$, 也就是对任意 x, 给出了一个与之对应的 a(a 对每个 x 也许不唯一, 但只要选择一个就够了), 即我们构造了 $\theta(x) = a, \theta \in \mathrm{Hom}(X, A)$. 此时 $i\theta = f$ 就是 $\mathrm{Ker}(p) \subseteq \mathrm{Im}(i)$. 于是 $\mathrm{Ker}(p) = \mathrm{Im}(i)$. □

上述表达中不要求正和列的最后以"0" 结尾, 也就是可能会出现: 原正和列 p 是满射, 但是对应的 p_* 不是满射的情况. 考虑商群 $\mathbb{Q}/\mathbb{Z}$, 以及其中的一个阶为 2 的元素 $1/2+\mathbb{Z}$, 这对应了一个二阶子群也就是 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2,\mathbb{Q}/\mathbb{Z})$ 非空. 对如下正合列作用 $\mathrm{Hom}(\mathbb{Z}_2,*)$ 函子:

$$0\to\mathbb{Z}\xrightarrow{i}\mathbb{Q}\xrightarrow{p}\mathbb{Z}/\mathbb{Q}\to 0$$

其中 i,p 分别为一般嵌入, 自然同态 (显然满射):

$$0\to\mathrm{Hom}(\mathbb{Z}_2,\mathbb{Z})\xrightarrow{i_*}\mathrm{Hom}(\mathbb{Z}_2,\mathbb{Q})\xrightarrow{p_*}\mathrm{Hom}(\mathbb{Z}_2,\mathbb{Z}/\mathbb{Q})\to 0$$

注意到 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2,\mathbb{Q}/\mathbb{Z})$. 非空以及 $\mathrm{Hom}(\mathbb{Z}_2,\mathbb{Q})=0$($\mathbb{Q}$ 中不含 2 阶元), 这反应了 p_* 绝对不会是满射.

定义 3.2.4. 对于模到 Abel 群上的函子 $T:_R\mathrm{Mod}\to\mathrm{Ab}$, 若是保证模的短正合列的左正合性不变的, 称为**左正合函子 (left exact functor)**, 即给出正和列:

$$0\to A\xrightarrow{i}B\xrightarrow{p}C$$

函子 T 作用后给出 Abel 群范畴中的正合列:

$$0\to T(A)\xrightarrow{T(i)}T(B)\xrightarrow{T(p)}T(C)$$

对于函子, 我们有对偶的构造—反变函子. 一个函子称为反变函子, 如果它把态射的箭头方向反转了. 具体定义如下.

定义 3.2.5 (反变函子 (contravariant functor)). (1) 对于 $\mathcal{C}$ 中的对象 $A\in\mathrm{obj}(A)$, $T(A)\in\mathrm{obj}(D)$.

(2) 对于态射 $f:A\to B$, 给出 $T(f):T(B)\to T(A)$.

(3) (结合律) 对于态射序列:

$$A\xrightarrow{f}A'\xrightarrow{g}A''$$

我们有: $T(A'')\xrightarrow{T(f)}T(A')\xrightarrow{T(g)}T(A)$ 满足:

$$T(gh)=T(h)T(g)$$

(4) (恒等态射)$\forall A\in\mathrm{obj}(C)$, $T(1_A)=1_{T(A)}$.

类似地, 我们有重要反变函子 $\mathrm{Hom}(*,X):_R\mathrm{Mod}\to\mathrm{Ab}$. 其中, 对于给定的两个对象 A,B, 任取 $f\in\mathrm{Hom}(A,B)$:

$$\begin{aligned}f^*:\mathrm{Hom}(B,X)&\to\mathrm{Hom}(A,X)\\ h&\to hf\end{aligned}$$

定理 3.2.6 ($\mathrm{Hom}(*, A)$ **的左正合性**)**.** *若有模上的正合列:*

$$A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

其中正合列在 $\mathrm{Hom}(*, X)$ *作用下构成 Abel 群的正合列:*

$$0 \to \mathrm{Hom}(C, X) \xrightarrow{p^*} \mathrm{Hom}(B, X) \xrightarrow{i^*} \mathrm{Hom}(A, X)$$

证明. 类似于前面的证明. □

注 34. 其中值得注意的一个点是, 对于原正合列 p 可能是满射, 但对应的 p^* 未必是单射. 我们还是考虑正合列:

$$0 \to \mathbb{Z} \xrightarrow{i} \mathbb{Q} \xrightarrow{p} \mathbb{Z}/\mathbb{Q} \to 0$$

考虑 $\mathrm{Hom}(*, \mathbb{Z})$ 函. 其中, 注意到 $\mathrm{Hom}(\mathbb{Q}, \mathbb{Z}) = 0$. 这是因为对于 $f : \mathbb{Q} \to \mathbb{Z}$ 给出 $f(a/b) = m \in \mathbb{Z}$, $nf(a/nb) = f(a/b) = m$. 这反应了 m 可被任意整数整除, 这意味着 $m = 0$. 而 $\mathbb{Z}$ 上的自同态一定是相当多的, 至少有 $1_{\mathbb{Z}}$. 所以从 p^* 绝不可能是满射.

类似, 我们有反变函子的左正合的概念:

定义 3.2.7. 设 T 是个反函子:$_R\,\mathrm{Mod} \to$, 给定正合列:

$$A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

其在函子作用下, 保持了正合性:

$$0 \to T(C) \xrightarrow{T(p)} T(B) \xrightarrow{T(i)} T(A)$$

称上述反变函子是**左正合 (left exact)** 的.

定理 3.2.8 (Hom **函子正合性的等价刻画**)**.** *设 $i : B' \to B$, $p : B \to B''$ 为 R 模上的同态, 对任意模 M 有正合列:*

$$0 \to \mathrm{Hom}(B'', M) \xrightarrow{p^*} \mathrm{Hom}(B, M) \xrightarrow{i^*} \mathrm{Hom}(B', M)$$

反过来会有如下正合列:

$$B' \xrightarrow{i} B \xrightarrow{p} B'' \to 0$$

证明. 充分抓住模 M 的任意性. 我们先取 $M = B''/\operatorname{Im} p$. 考虑自然态射:

$$f : B'' \to B''/\operatorname{Im} p$$

在 p^* 作用下, 可以得到 $fp : B \to B''/\operatorname{Im} p$. 显然有 $fp = 0$, 而借助 p^* 的正合性 (Hom 正合列得出), 我们得 $f = 0$. 此时也就是 $\operatorname{Im} p = B''$.

其次, 取 $M = B''$, 取 $1_{B''} \in \mathrm{Hom}(B'', B'')$, 分别在 p^*, i^* 作用下得到:

$$i^*p^*1_{B''} = (pi)^*1_{B''} = 0$$

由此得到 $i^*p^*1_{B''} = 0 = ip1_{B''} = ip$, 即 $\mathrm{Im}\, i \subseteq \mathrm{Ker}\, p$.

最后取 $M = B/\mathrm{Im}\, i$, $h : B \to M$ 为自然态射. $hi = 0$, 从而有 $i^*h = 0, h \in \ker i^*$, 于是存在 $h' : B'' \to M, p^*h' = h'p = h$. 至此, 我们已证 $\mathrm{Im}\, i \subset \mathrm{Ker}\, p$, 若是 $\mathrm{Im}\, i \neq \mathrm{Ker}\, p$, 则存在 $b \in B$, 且 $b \notin \mathrm{Im}\, i, b \in \mathrm{Ker}\, p$. 此时 $hb \neq 0$, $pb = 0$ 而 $h'pb = hb = 0$, 矛盾. □

定义 3.2.9 (**双模 (bimodule)**)**.** 若 M 是一个 Abel 加群, 在此之上分别定义了左 R 模和右 S 模, 且他们通过结合律联系:

$$r(ms) = (rm)s$$

其中, $r \in R, m \in M, s \in S$. 此时称 M 为 $(R, S)-$ 双模, 记作 ${}_RM_S$.

定理 3.2.10 (**双模结构上可定义 Hom 集的模结构**)**.** *设一双边模 ${}_RA_S$, 以及单纯的左 R 模 B, 就有如下函子:*

$$\mathrm{Hom}_R(A, *) :_R \mathrm{Mod} \to_S \mathrm{Mod}$$

证明. $\mathrm{Hom}(A, B)$ 可以在上面构造出左 S 模结构:

$$sf(x) = f(xs)$$

验证, 诸如 $s_1(s_2f(x)) = s_1f(xs_2) = f(x(s_1s_2)) = (s_1s_2)f(x)$ 以及相应的加法分配律即可. 在这种左 S 模结构下, 我们需说明对于态射 $f :_R A \to_R B$ 构成 S 同态: $\mathrm{Hom}(A, B) \to \mathrm{Hom}(A, B')$. 此时只需注意到如下关系即可:

$$g_*(sf(x)) = g_*(f(xs)) = gf(xs) = sgf(x) = s(g_*f(x))$$

□

推论 3.2.11. *设一交换环 R, 以及相应的 A, B 左 R 模, 则 $\mathrm{Hom}(A, B)$, 在定义运算 $rf(x) = f(rx)$ 下可构成 R 模, 然后就诱导出函子 $\mathrm{Hom}(A, *) :_R \mathrm{Mod} \to_R \mathrm{Mod}$.*

证明. 事实上, 对于交换环 R 上的模, 定义运算 $(m, r) = rm$. 因为可以导出一种双边模 ${}_RM_R$, 注意到 $rf(x) = f(xr) = f(rx)$, 我们不难证明以上推论. □

推论 3.2.12. *设 R 为一个环, M 是左 R 模, 则 $\mathrm{Hom}(R, M)$ 构成一个左 R 模, 且有同构:*

$$\phi_M : f \mapsto f(1)$$

证明. 首先, 注意到 R 关于自身是构成双模的 (不用再定义 $rm = mr$ 之类, R 未必是交换的). 按上文定义的方式: $rf(x) = f(xr)$. 我们在 $\mathrm{Hom}(R, M)$ 上定义了一种 R 模. 其次, 对于 $\phi_M : \mathrm{Hom}(R, M) \to M$, 容易验证:

$$r\phi_M(f) = rf(1) = \phi_M(rf) = f(1r) = f(r)$$

不难验证其保持加法性质, 于是 ϕ_M 构成 R 同态. 考虑映射:

$$\Phi : M \to \mathrm{Hom}(R, M)$$
$$m \to f_m$$

其中 $f_m(r) = rm$. 可以验证 $\Phi\phi_M(f) = \Phi f(1) = g_{f(1)} = f$, 其中:

$$g_{f(1)}(r) = rf(1) = f(1r) = f(r)$$

反之同理可得, 由此 Φ_M 为同构. □

定理 3.2.13 (协变 Hom 函子保持积 (正向极限)). *若存在双模 ${}_RA_S$, 以及一系列的左 R 模, 则存在 S 同构:*

$$\phi : \mathrm{Hom}(A, \prod B_i) \cong \prod \mathrm{Hom}(A, B_i)$$

其中 $\phi : f \mapsto (p_i f), p_i$ 是投影映射.

证明. $\prod B_i$ 是 R 模, 则 $\mathrm{Hom}(A, \prod B_i)$ 上可以构造出一个 S 模. 同样 $\prod \mathrm{Hom}(A, B_i)$ 可以构成 S 模. 我们把 $f(a) = (f_1(a), f_2(a), \dots)$ 记为 $(f_1, f_2, \dots)(a)$, 其中 $f_1 = p_1 f$. 也就是上述的同构成立. 顺承上述思路, 显然的构造 $\phi : f \mapsto (p_i f)$, 考察:

$$s\phi(f) = s(p_i f) = (sp_i f)$$

上式后一个等号成立是模运算的定义. 另一边 $\phi(sf) = (p_i(sf))$, 我们需要说明每个分量满足 $s(p_i f) = p_i(sf)$. 取 $a \in A$,

$$p_i(sf)(a) = p_i(f(as)) = (p_i f)(as) = s(p_i f)(a)$$

于是, ϕ 构成 S 同态. 对于同构, 不难看出 $\phi(f) = 0$, 也就是 $\mathrm{Ker}(\phi) = 0$. □

3.3 Galois 理论简介

Galois 理论是对于代数学的发展有重要推动作用. 本节内容主要涉及: 1. 回顾五次一般方程不可解问题, 将问题转化为域论中根式扩域问题; 采用群论的语言, 讨论根式扩域与 Galois 群的关系 (正规扩域与 Galois 群, 简介可解群的产生, 可解的群性质和

Jordan—Holder 定理). 2. 证明 Galois 定理和 Abel—Ruffini 定理: 五次一般方程不可根式求解. 3. Galois 扩张的产生和 Galois 对应, 分别从范畴和格的语言看待 Galois 对应. 4. 作为正向 (反向) 极限的例子, 简介无限 Galois 对应; 绝对 Galois 群和可分代数闭包. 5. 低维 Galois 群的计算.

3.3.1 n 次一般方程不可解问题

Galois 理论, 也成为方程论 (Theory of Equations), 起源于 n 次一般方程的求解问题. n 次一般方程求解问题等价于为域论中的 n 次一般方程根式扩域的存在问题. 利用多项式的 Galois 群, 可将 n 次一般方程根式扩张存在问题转化为 Galois 群是否可解的群论问题之间的关系, 这也是可解群的产生原因之一.

首先, 我们指出任意域上的多项式非常值都有根.

定理 3.3.1 (Kronecker 定理). *k 为一个域, $f(x) \in k[x]$, 则存在域扩张 K/k, 使得 $f(x)$ 在域 k 上可表示为一次多项式 (线性式) 的乘积:*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - z_1)\cdots(x - z_n)$$

其中, $z_1, z_2, \ldots, z_n \in K$ 均为 $f(x)$ 的根.

证明. 对多项式的次数进行归纳. 设 $f(x) \in k[x]$, 当 $\deg(f) = 1$ 时, $f(x)$ 为线性多项式, 令 $K = k$ 即可. 当 $\deg(f) = n > 1$ 时, 若 $f(x)$ 是可约多项式, 则存在不可约多项式 $p(x) \in k[x]$, 使得 $f(x) = p(x)g(x)$. 由归纳法, $\deg(p(x)) \leq n, \deg(g(x)) \leq n$, 存在 K_1, K_2 使得 p, g 可完全分解. 令 $K = \langle K_1 \cup K_2 \rangle$, $f(x)$ 在 K 上可完全分解. 若 $f(x)$ 为不可约多项式, 则根据多项式环构造代数扩张定理, $k[x]/(f(x))$ 为 k 的扩域, 记为 F. $x + f(x)$ 为 $f(x)$ 的根, 记为 u. $F \cong k(u)$. 于是, 在域 F 上的多项式环 $F[x]$ 中, 存在分解 $f(x) = (x - u)h(x)$, 其中 $h(x) \in F[x]$, $\deg(h(x)) < n$, 由归纳法, 存在 F 的扩域 K, 使得 $f(x)$ 完全分解为一次因式. □

注 35. 对于 Kronecker 定理, 我们有如下说明:

(1) 从 Kronecker 定理, 我们可以直接推得分裂域的存在性. 事实上, 我们在证明分裂域的存在性, 也证明了 Kronecker 定理.

(2) Kronecker 定理可进一步推广为: 任何一个域 k, 都是其某个代数封闭域的子域.

定义 3.3.2. k 是一个域, $E = k(y_1, y_2, \ldots, y_n) = \mathrm{Frac}(k[y_1, y_2, \ldots, y_n])$ 为域 k 的 n 元有理函数域. 若

$$f(x) = \prod_i (x - y_i) \in E[x]$$

则称 $f(x)$ 为**域 k 上的 n 次一般多项式** (general polynomial of degree n over k). 进一步地,

$$f(x) = (x - y_1)(x - y_2)\cdots(x - y_n) = x^n + a_{n-1}x^{n-1} + \cdot + a_0$$

$a_i = a_i(y_1, y_2, \cdots, y_n) \in E$. 在不计正负号的意义下, 称 a_i 为 n **元初等对称函数** (elementary symmetric functions).

例 3.3.3. 域 k 上的二次一般多项式为:

$$f(x) = (x - y_1)(x - y_2) = x^2 - (y_1 + y_2)x + y_1y_2$$

其中, 二元初等对称函数为 $a_0 = a_0(y_2, y_2) = y_1y_2$; $a_1 = a_1(y_2, y_2) = -(y_1 + y_2)$.

类似上述例子, 我们可以写出 n 元初等对称函数

$$f(x) = (x - y_1)(x - y_2)\cdots(x - y_n) = x^n + a_{n-1}x^{n-1} + \cdot + a_0$$

显示表达式 (不计正负号):

$$\begin{cases} a_{n-1} = \sum\limits_{i=1}^{n} y_i \\ a_{n-2} = \sum\limits_{i<j} y_iy_j \\ a_{n-3} = \sum\limits_{i<j<k} y_iy_jy_k \\ \cdots \\ a_0 = \prod\limits_{i=1}^{n} y_i \end{cases}$$

特别地, 若 $f(x) \in E[x], E = \mathrm{Frac}(k)$ 是域 k 上的 n 次一般多项式, 则 $\sum\limits_{i}^{n} y_{i=1} \in k$, $\prod\limits_{i=1}^{n} y_i \in k$.

下面, 我们阐述 n **次一般方程根式求解问题**:

k 为一个域, $f(x) \in k[x]$, 由 Kronecker 定理, 存在域扩张 K/k 使得, $f(x)$ 可完全分解为一次线性式的乘积:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdot + a_0 = (x - y_1)(x - y_2)\cdots(x - y_n)$$

令 $E = k(y_1, y_2, \ldots, y_n), F = k(a_0, a_2, \cdots, a_{n-1})$, 则 $f(x)$ 为域 k 上 n 次一般多项式, 即 $f(x) \in E[x]$, E/F 是 $f(x)$ 的分裂域. 由根与系数的关系 (初等对称函数的由来), 我

们有如下方程系统:

$$Equ.\quad System\begin{cases} a_{n-1}=-\sum\limits_{i=1}^{n}y_i=e_1(z_1,z_2,\cdots,z_n) \\ a_{n-2}=\sum\limits_{i<j}y_iy_j=e_2(z_1,z_2,\cdots,z_n) \\ a_{n-3}=-\sum\limits_{i<j<k}y_iy_jy_k=e_3(z_1,z_2,\cdots,z_n) \\ \cdots \\ a_0=(-1)^n\prod\limits_{i=1}^{n}y_i=e_n(z_1,z_2,\cdots,z_n) \\ e_j(z_1,z_2,\cdots,z_n)=(-1)^ja_{n-j}, j=1,2,\ldots,n. \end{cases}$$

域 k 上的 n 次一般方程 $f(x)\in E[x]$ 根式求解问题是: 如何通过域 F 上的算子 (加, 减, 乘, 除) 及开方运算求解上述方程系统, 使得用多项式的系数表示出多项式的根.

对于 n 次一般方程根式求解的问题, 已经完全得到解决. 当 $n=2$ 时, 我们有二次求根公式 (quadratic formula); 当 $n=3$ 时, 我们有三次求根公式 (cubic formula) 和四次求根公式 (quantic formula). 当 $n\geq 5$ 时, 我们没有类似求根公式的结果, 但通过借助其他算子, 我们可以找到 n 次一般方程的一些解:

(a) Newton 迭代法 (分析学): r 为 $f(x)$ 的实根, x_0 是 r 的一个近似 (给定精度), 通过迭代

$$x_{n+1}=x_n-\frac{f(x_n)}{f'(x)};\ \lim_{n\to\infty}x_n=a$$

a 为 n 次一般方程的一个解. 这也是动力系统 (dynamical system) 的基本方法之一.

(b) Hermite 对于 5 次方程求解使用了代数几何中的椭圆模函数 (elliptic modular function).

(c) 对于高次多项式的求根, 我们可使用超几何函数 (hypergeometry function), 这是属于双曲几何的内容.

(d) Abel 在 1824 年证明了: 5 次及 5 次以上的一般方程不可根式求解. Ruffini 在 1799 年证明了与 Abel 相同的结果, 但 Ruffini 的证明复杂且长, 没能得到同时期数学家的认可. 它们的证明关键之处都是洞察到了" 对称性" 的存在.

在第二章第四节 Luroth 定理中, 我们已经引入过 $k-$ **自同构**和**域扩张的 Galois 群**的概念. 下面, 我们讨论一些 $k-$ 自同构的性质, 给出多项式的 Galois 群, 并指出在同构的意义下, 多项式的 Galois 群与其分裂域的 Galois 群是相统一的.

性质 3.3.4. *k 是一个域, $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in k[x]$, 设 $\{z_1,z_2,\cdots,z_n\}$ 为 $f(x)$ 的 n 个根. $E=k(z_1,z_2,\cdots,z_n)$ 是 $f(x)$ 的分裂域, 若 $\sigma\in \mathrm{Aut}(E)$ 为 $k-$ 自同构, 则 σ 限制在集合 $\{z_1,z_2,\cdots,z_n\}$ 上为一个置换. 即 σ 把根映成根.*

证明. z 为 $f(x)$ 的一个根, 则

$$0 = f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$$

对于任意 $\sigma \in Gal(E/k)$, 考虑 σ 作用到方程两侧得:

$$0 = \sigma(0) = \sigma(z^n) + \sigma(a_{n-1})\sigma(z^{n-1}) + \cdots + \sigma(a_1)\sigma(z_1) + \sigma(a_0)$$

因为 $\sigma_{|k} = Id_k$

$$0 = \sigma(z)^n + a_{n-1}\sigma(z)^{n-1} + \cdots + a_1\sigma(z) + a_0 = f(\sigma(z))$$

即 $\sigma(z)$ 也是 $f(x)$ 的根, 故 σ 限制在根集上为置换. □

注 36. $f(x) \in k[x]$ 是域 k 上的多项式, Ω 为 $f(x)$ 所以零点. σ 为 $k-$ 自同构, 则 $\sigma_{|\Omega} : \Omega \mapsto \Omega$ 为集合 Ω 的置换. 于是, 我们可以定义映射:

$$\Theta : \mathrm{Gal}(E/k) \mapsto S_n$$

$$\sigma \mapsto \Sigma_\sigma := \begin{pmatrix} z_1 & z_2 & \cdots & z_n \\ \sigma(z_1) & \sigma(z_2) & \cdots & \sigma(z_n) \end{pmatrix}$$

其中 $z_1, z_2, \cdots, z_n$ 为 $f(x)$ 的根.

定义 3.3.5. k 是一个域, $f(x) \in k[x]$, E 是 $f(x)$ 的分裂域. 令 $G_f := \{\Sigma_\sigma | \sigma \in Gal(E/k)\}$, 称 G_f 为**多项式 $f(x)$ 的 Galois 群**.

下面一个定理指出: 多项式的 Galois 群和分裂域的 Galois 群在同构意义下是相容的, 这也是早期 Galois 定义的 Galois 群, 后面我们发现 Galois 群的讨论采用域的语言更具有一般性, 因为它不依赖于多项式.

引理 3.3.6. *E/k 是一个域扩张, $E = k(z_1, z_2, \cdots, z_n)$. 若 $\sigma \in \mathrm{Gal}(E/k)$, $\sigma(z_i = z_i)$, 则 $\sigma = 1_E$.*

证明. 对元素个数 n 采用归纳法. 当 $n = 1$ 时, 对于 $\forall u \in E$, 存在 $f(x), g(x) \in k[x]$, 使得

$$u = \frac{f(z_1)}{g(z_1)}$$

当 σ 保持 k 上元素和 z_1. 即 $\sigma(u) = u$, 当 $n \geq 1$ 时, 类似可得. □

定理 3.3.7 (多项式的 Galois 群同构于分裂域的 Galois 群). *$f(x) \in k[x]$, $\deg(f(x)) = n$, E 是 $f(x)$ 的分裂域, 则 $\mathrm{Gal}(E/k) \cong G_f \leq S_n$.*

证明. 令 $\Omega = \{z_1, z_2, \cdots, z_n\}$ 为 $f(x)$ 的所有根构成的集合. 对于 $\forall \sigma \in \operatorname{Gal} E/k$, $\sigma_{|\Omega}$, 由此, 我们可定义

$$\begin{aligned} \varphi: \quad & \operatorname{Gal}(E/k) \mapsto S_\Omega \\ & \sigma \mapsto \Sigma_\sigma \end{aligned}$$

容易验证 φ 是一个群同态, 这是因为

$$\varphi(\sigma\gamma) = \Sigma_{\sigma\gamma} = \Sigma_\sigma \Sigma_\gamma = \varphi(\sigma)(\gamma)$$

根据上述引理: $\operatorname{Ker}\varphi = \{1\}$. 故

$$\operatorname{Im}\varphi = G_f \cong \operatorname{Gal}(E/k)$$

□

例 3.3.8. $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, 令 $E = \mathbb{Q}(i)$, 则

$$\operatorname{Gal}(E/\mathbb{Q}) \cong G_f \leq S_2 \cong \mathbb{Z}_2$$

因为复共轭 $\sigma : a \mapsto \overline{a}$ 为 $\mathbb{Q}-$ 自同构, 故 $G = \langle\sigma\rangle \cong \mathbb{Z}_2$.

下面, 我们将上述 n 次一般方程根式求解问题转化为域论的问题. 域论的语言, 对于一般根式方程求解问题的刻画是十分直观的.

定义 3.3.9. k 是一个域, 称域扩张 $K(u)/k$ 为一个 m **型纯扩张** (pure extension of type m), 若存在 $m \in \mathbb{Z}, u^m \in k$.

定义 3.3.10. 称一个域扩张 K/k 为**根式扩张** (radical extension), 若存在一个存扩张塔:

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = K$$

其中 K_{i+1}/K_i 为纯扩张.

定义 3.3.11. $f(x) \in k[x]$, E/k 为 $f(x)$ 的分裂域. 称 $f(x)$ 为**根式可解的** (solvable by radicals), 若存在根式扩张 K/k :

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = K$$

使得 $E \subseteq K_t$.

注 37. 关于上述三个定义, 我们做如下说明:

(1) m 型纯扩张 $k(u)/k$ 是在域 k 上添加了某元素 $a \in k$ 的一个 m 次单位根. 如果域 k 包含了所有的 m 次单位根, 则 m 型纯扩张 $k(u)/k$ 是多项式 $x^m - a$ 的分裂域. 但并非所有的域 k 都包含 m 次单位根, 例如有理数域 $\mathbb{Q}$.

(2) 根式扩张等价于存在一个纯扩张塔.

(3) 任意一个 m 型纯扩张 $k(u)/k$, $m = p_1p_2\cdots p_q$, p_i 是素数, 都等价于一个纯扩张塔

$$k \subseteq k(u^{\frac{m}{p_1}}) \subseteq k(u^{\frac{m}{p_1p_2}}) \subseteq \cdots \subseteq k(u)$$

例如, $k(u)/k$ 是 6 型纯扩张, $u^6 = (u^3)^2 \in k$, 我们有存扩张塔 $k \subseteq k(u^3) \subseteq k(u)$. 素因子分解定理自然诱导出纯扩张塔.

(4) $f(x) \in k[x]$ 为根式可解的, 等价于仅 $f(x)$ 各项系数仅使用域上算子及开方运算可以表示出 $f(x)$ 的根. 这是因为, $f(x)$ 根式可解等价于存在纯扩张塔:

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = K$$

使得 $E \subseteq K_t$, E/k 是分裂域. 纯扩张塔等价于: z 为 $f(x)$ 的根, $z \in E \subseteq K_t = K_{t-1}(u)$, $u^m = \alpha \in K_{t-1}$, 即 z 可以用 K_{t-1} 上的元素元素和 $\alpha \in K_{t-1}$ 的开方表示. $K_{t-2} = k_{t-1}(v)$, z 可以用 K_{t-2} 上的元素运算和开方表示. 以此类推, z 可以被域 k 上的元素经过加, 减, 乘, 除, 开方表示.

例 3.3.12. 下面, 我们给出一些可根式求解的例子.

(a) k 是一个域, $f(x) = x^n - 1$ 为根式可解的, 对于任意的 $n \in \mathbb{N}^+$, 设 ω 为 n 次本原单位根, $E = k(\omega)$ 为 $f(x)$ 的分裂域, $E = k(\omega)/k$ 为一个根式扩张.

(b) p 是素数, k 为包含所有 p 次单位根的域. 如果 $k(u)/k$ 为 p 型纯扩张, 当 $\operatorname{Char} k = 0$ 或者 $\operatorname{Char} k = p$ 时, $k(u)/k$ 为多项式 $f(x) = x^p - u^p$ 的分裂域, 从而其根式可解. 当 $\operatorname{Char} k \neq p$, $f(x)$ 为可分多项式: $f(x) = \prod\limits_i (x - \omega^i u)$, 其中 ω 为 p 次本原单位根, $k(u)/k$ 是分裂域.

(c) 对于二次方程 $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$, 其根为:

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

令 $k = \mathbb{Q}(b, c)$, $K_1 = k(u)$, 其中 $u = \sqrt{b^2 - 4c}$, $u^2 \in k$,K_1 为分裂域, K_1/k 是根式扩张. 于是 $f(x)$ 可根式求解.

下面, 我们采用群论的语言, 对于 n 次一般方程根式求解问题进行研究. 我们已经知道域多项式的 Galois 群同构于多项式分裂域的 Galois 群, 通过分裂域的 Galois 群, 我们可以得到多项式根式可解性.

首先, 我们引入正规扩张和可解群的概念, 它们是研究多项式 Galois 群和根式扩张关系的重要桥梁和工具, 也正因如此, 可解群和正规扩张产生并成为重要研究对象.

定义 3.3.13. 称域扩张 E/k 是**正规扩张** (normal extension), 如果存在多项式 $f(x) \in k[x]$, 使得 E 为 $f(x)$ 的分裂域.

注 38. E/k 是正规扩张当且仅当, 任何不可约多项式 $p(x) \in k[x]$ 存在一根在 E 中, 则所有的根在 E 中. 这个证明不是显而易见的, 可参考《近世代数基础》刘绍学 (第二版) 的正规扩张一节. 基域 k 包含所有 n 次单位根, 则 n 次纯扩张为正规扩张.

例 3.3.14. $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $E = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ 为 $f(x)$ 的分裂域. 其中,

$$\mathbb{Q}(e^{\frac{2\pi i}{3}})/\mathbb{Q}是正规扩张, x^3 - 1的分裂域$$

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}不是正规扩张$$

下面的定理是正规扩张重要的性质, 也是联系 Galois 群与多项式根式可解基本理论之一.

定理 3.3.15 (正规扩域塔的 Galois 群). *$k \subseteq B \subseteq E$ 为域扩张塔, B/k 和 E/k 为正规扩张, 则对于任意的 $\sigma \in \mathrm{Gal}(E/k), \sigma(B) = B$, 且*

$$\mathrm{Gal}(E/B) \triangleleft \mathrm{Gal}(E/k)$$

$$\mathrm{Gal}(E/k)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k)$$

证明. 因为 B/k 是一个正规扩张, 则存在 $f(x) \in k[x]$, B 是 $f(x)$ 的分裂域. 设 $f(x)$ 的根为 $\{z_1, z_2, \cdots, z_n\}$, $B = k(z_1, z_2, \cdots, z_n) \subseteq E$. 对于任意的 $\sigma \in \mathrm{Gal}(E/k)$, $\sigma_{|B}$ 是 $B-$ 自同构. 所以 $\sigma(B) = B$. 定义映射:

$$\begin{aligned} \rho: \quad \mathrm{Gal}(E/k) &\mapsto \mathrm{Gal}(B/k) \\ \sigma &\mapsto \sigma_{|_B} \end{aligned}$$

ρ 为满同态, 且 $\mathrm{Ker}\,\rho = \{\sigma | \sigma_{|_B} = Id\} = \mathrm{Gal}(E/B) \triangleleft \mathrm{Gal}(E/k)$. 于是,

$$\mathrm{Gal}(E/k)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k)$$

□

下面定理中, 我们给出了根式扩张和 Galois 群的对应: E/k 根式扩张诱导出了 $\mathrm{Gal}(E/k)$ 的子群序列.

定理 3.3.16 (根式扩张的 Galois 群). *$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$ 是纯扩张塔, 其中 K_i/K_{i-1} 是素数 p_i 型纯扩张 (任意纯扩张塔总可分解成该形式). 如果 K_t/k 为正规扩张, 且 k 包含所有的 p_i 次单位根 $(i = 1, 2, \ldots, t)$, 则存在一个 Galois 群的子群序列:*

$$\mathrm{Gal}(K_t/k) = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_t = \{1\}$$

其中, G_i/G_{i+1} 要么是为 p_{i+1} 阶素数群, 要么是 {1}.

证明. 参见 Rotman 英文原版书籍 *Advanced Algbra* Lemma A-5.19. Page. 192 . □

从上述引理, 我们可以引出可解群的概念, 下面我们列出可解群一些基本性质和重要结果. 在研究可解群过程当中, 我们借助了群的合成序列这一有力的刻画工具, 下面给出合成序列的定义, 它和模的合成序列的定义类似.

定义 3.3.17. G 是一个群, 称群 G 的**正规子群列** (normal sequence) 为:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = \{e\}$$

商群组 $G_0/G_1, G_1/G_2, \cdots, G_{r-1}/G_r$ 为**因子群组** (factor groups). 非平凡的因子群的个数称为正规子群列的**长度** (length).

定义 3.3.18. G 是一个群, 群 G 的**合成序列** (composition sequence) 是指一个正规子群列:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = \{e\}$$

其中的因子群组为单群:G_i/G_{i+1} 为单群. 称非平凡的因子群称为 G 的**合成因子** (composition factors), 称非平凡的因子群的个数称为 G 的**合成序列的长度** (composition length).

引入合成序列后, 一个自然的问题是: 什么样的群具有合成序列; 同一个群不同的合成序列具有的什么关系. 下面, 我们回答这两个问题.

性质 3.3.19. *每一个有限群 G 都有合成序列.*

证明. 参见 Rotman 英文原版书籍 *Advanced Algbra* Proposition A-5.27. Page. 195 . 或者参考丘维声《近世代数》北京大学出版社第 65 页之命题 5. □

下面, 我们直接给出可解群的等价刻画, 其中 (2) 为可解群的通常定义.

定理 3.3.20 (**可解群的等价定理**)**.** *G 是一个群, 则以下等价:*

(1) G 为可解群.

(2) 存在 $k \in \mathbb{Z}^+$, 群 G 的 k 阶导群 (换位子群)$G^k = \{e\}$.

(3) 存在 G 的正规子群列:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s = \{1\}$$

且因子群组 G_i/G_{i+1} 为 Abel 群.

(4) 存在 G 的合成序列:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s = \{1\}$$

其因子群组为素数阶循环群. (有限 Abel 群是单群当且仅当, 它是素数阶循环群).

证明. (2) $\Longleftrightarrow$ (3) 参见丘维声《近世代数》北京大学出版社第 62 页之定理 1.
(3) $\Longleftrightarrow$ (4) 参见 Rotman 英文原版书籍 *Advanced Algbra* Exercise A-5.9(ii). Page. 200 . □

下面, 我们给出关于可解群的一些性质, 它在判断多项式的 Galois 群是否可解时具有重要作用.

定理 3.3.21 (可解群的性质).

(1) *Abel 群为可解群. 非交换单群不为可解群. 奇数阶群都是可解群 (W.Feit — J.Thompson Theorem). 非交换单群都是偶数阶群.*

(2) $S_n(n \geq 5)$ 不是可解群, 这是因为 $A_n(n \geq 5)$ 是非交换单群. S_4 为可解群, 我们有合成序列:

$$S_4 \triangleright A_4 \triangleright V \triangleright \{(12)(34), (1)\} \triangleright \{1\}$$

其中, $\boldsymbol{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$ 为四群 *(four group)*, 即 4 阶二面体群 *(dihedral group)*.

(3) 可解群的子群及同态像都是可解群.

(4) 可解群的商群为可解群.

(5) G 是一个群, $N \triangleleft G$, N 和 G/N 是可解群, 则 G 是可解群.

(6) 可解群的内直积为可解群.

(7) (Burnside) 定理: G 是有限群, 若 $|G| = p^m q^n$, p, q 均为素数, 则 G 为可解群.

证明. (3), (4), (5) 的证明可参考 Rotman 英文原版书籍 *Advanced Algebra* Proposition A 5.22, 5.23, 5.25. Page. 193—194. 或者参考丘维声《近世代数》北京大学出版社第 62—63 页之定理 2, 定理 3, 推论 1.
(6) 的证明可参考 Rotman 英文原版书籍 *Advanced Algbra* Corollary A– 5.26. Page. 195.
(7) 的证明可参考 Rotman 英文原版书籍 *Advanced Algebra* Theroem C—2.59 .Part II .Page. 168. □

同样的, 类似于模的合成序列, 我们有 Zassenhaus 引理和 Schreier 加细定理.

定义 3.3.22. G 是一个群, 称 G 的两个正规子群列**等价**, 若存在两者间非平凡因子群的双射, 且双射诱导相应的因子群同构.

定义 3.3.23. 一个正规子群列的**加细** (refinement) 是把原始的正规子群列作为子序列的正规子群列.

定理 3.3.24 (Schreier 加细定理). *群 G 任意两个正规子群列*

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s = \{1\}$$

$$G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \cdots \triangleright N_r = \{1\}$$

都有等价的加细.

证明. 参见 Rotman 英文原版书籍 *Advanced Alegbra* Theorem A-5.29. Page. 197 . □

最后, 我们介绍群论中的 Jordan—Holder 定理, 它给出了关于群的不变量.

定理 3.3.25 (Jordan—Holder). *群 G 的任意合成序列等价. 特别的, 如果合成序列存在, 合成序列的长度为群 G 的*__不变量__ *(invariant).*

证明. 参见 Rotman 英文原版书籍 *Advanced Algebra* Theorem A-5.30. Page. 198 . □

合成序列长度 2, 因子群为 $\mathbb{Z}_2, \mathbb{Z}_2$, 但 $\mathbb{Z}_{\not 2} \ncong \mathbf{V}$.

注 39. 合成序列的长度不是群的完全不变量. 例如, 存在 $\mathbb{Z}_4$ 和 $\mathbf{V}$ 两个群,

$$\mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$$

同构意义下, 它们具有等价的合成序列, 但 $\mathbb{Z}_4 \ncong V$.

最后, 我们用可解群的语言描述根式扩张的 Galois 群.

定理 3.3.26 (多项式根式可解的 Galois 群). *k 是一个域, $f(x) \in k[x]$ 根式可解, E/k 是 $f(x)$ 的分裂域. $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$ 是纯扩张塔, 其中 K_i/K_{i-1} 是素数 p_i 型纯扩张 (任意纯扩张塔总可分解成该形式). 如果 $E \subseteq K_t$, 且 k 包含所有的 p_i 次单位根 $(i = 1, 2, \ldots, t)$, 则 Galois 群 $\mathrm{Gal}(E/k)$ 是某个可解群的商群, 也是可解群.*

证明. K_t/k 是某个多项式的分裂域, 故 K_t/k 是正规扩张. 于是 $\mathrm{Gal}(K_t/k)$ 是可解群. 注意到 $k \subseteq E \subseteq K_t$, E/k 是分裂域, 故为正规扩张. 于是

$$\mathrm{Gal}(K_t/k)/\mathrm{Gal}(K_t/E) \cong \mathrm{Gal}(E/k)$$

于是 $\mathrm{Gal}(E/k)$ 是可解群. □

3.3.2 Galois 定理和 Abel—Ruffini 定理

经过可解群, 根式扩张等一系列的准备, 现在我们可以对 n 次一般方程给出完美的回答. 同时, 我们还给出一般域 k 上多项式可根式求解的刻画定理.

首先, 我们考察域 k 上 m 次分圆多项式的 Galois 群.

引理 3.3.27. *k 是一个域, $m \in \mathbb{N}^+$, E 是域 k 上 m 次分圆多项式 $x^m - 1$ 的分裂域, 则 $\mathrm{Gal}(E/k)$ 是 Abel 群. 事实上, $\mathrm{Gal}(E/k)$ 同构于 $\mathrm{U}(\mathbb{Z}_m) = \{[i] \in \mathbb{Z}_m \mid \gcd(i, m) = 1\}$.*

证明. 参考 Rotman 英文原版书籍 *Advanced Algebra* Proposition A.5-12 .Part I .Page. 186. □

定理 3.3.28 (Galois 定理). *k 是一个域, $f(x) \in k[x]$, E/k 是 $f(x)$ 的分裂域, 若 $f(x)$ 可根式求解, 则 $\mathrm{Gal}(E/k)$ 是可解群.*

注 40. 当 $\mathrm{Char}\, k = 0$ 时, 上述命题的逆命题也成立. $\mathrm{Char}\, k = p$, p 是素数时, 逆命题不成立, 对此我们有反例: p 是素数, $k = \mathbb{F}_p(t)$, $f(x) = x^p - x - t \in k[x]$, 其 Galois 群是 p 阶循环群, 但是 $f(x)$ 在域 k 上不可根式求解. 具体参考 Rotman 英文原版书籍 *Advanced Algebra* Theorem A-5.66. Page. 220.

证明. $f(x)$ 根式可解, 则存在根式扩张 (纯扩张塔):

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t$$

其中, K_t/K_{t-1} 为素数 p_t 型纯扩张, $E \subseteq K_t$. 令 $m = p_1 p_2 \cdots p_t$, 定义 E^* 为域 E 上多项式 $x^m - 1$ 的分裂域. 令 Ω 为 E^* 上所有的 m 次单位根组成的集合.

$$\Omega = \{a \in E^* \mid a^m - 1 = 0\}$$

令 $k^* = k(\Omega)$. E^*/k^* 为正规扩张, $(x^m - 1)f(x)$ 为 k^* 的分裂域. k^*/k 是正规扩张, 它是域 k 上多项式 $x^m - 1$ 的分裂域. 考察域扩张塔: $k \subseteq k^* \subseteq E^*$, 根据正规扩张 Galois 群的性质知:

$$\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/k^*) \cong \mathrm{Gal}(k^*/k)$$

其中, m 次分圆多项式 $\mathrm{Gal}(k^*/k)$ 是 Abel 群, 从而是可解群. 而 k^* 包含了所有的 $p_i (i = 1, 2, \cdots, t)$ 次单位根, 且 $k^* \subseteq E \subseteq E^*$, E^*/k^* 是多项式 $f(x)$ 在 k^* 上的分裂域. 于是 $\mathrm{Gal}(E^*/k^*)$ 为某个可解群的商群, 也是可解群. 于是 $\mathrm{Gal}(E^*/k)$ 是可解群. 考虑 $k \subseteq E \subseteq E^*$, E/k 是正规扩张, 为 $f(x)$ 的分裂域; E^*/k 是正规扩张, 为 $(x^m - 1)f(x)$ 的分裂域. 于是,

$$\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/E) \cong \mathrm{Gal}(E/k)$$

可解群的商群是可解群, 于是 $\mathrm{Gal}(E/k)$ 是可解群. □

定理 3.3.29 (Abel—Ruffini 定理). *k 为一个域,*

$$E = k(y_1, y_2, \cdots, y_n) = \mathrm{Frac}(k[y_1, y_2, \cdots, y_n])$$

为 k 的 n 元有理函数域. k 上的 n 次一般方程

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdot + a_0 = (x - y_1)(x - y_2)\cdots(x - y_n)$$

当 $n \geq 5$ 时, $f(x)$ 不可根式求解.

证明. 令 $F = k(a_0, a_1, \cdots, a_{n-1})$, 则 E/F 是 $f(x)$ 在 F 上的分裂域. 我们断言:

$$\mathrm{Gal}(E/F) \cong S_n$$

n 次多项式的 Galois 群同构于 n 阶置换群的某个子群, 于是:

$$\mathrm{Gal}(E/F) \leq S_n$$

下面, 我们证明:

$$|\mathrm{Gal}(E/F)| \geq |S_n|$$

我们注意到一个**事实**:A, R 均为整环, $A \cong R$. $\sigma : A \mapsto R$ 是环同构, 则 σ 可唯一开拓为分式域的同构:

$$\begin{gathered}\Psi : \mathrm{Frac}(A) \mapsto \mathrm{Frac}(R) \\ \tfrac{a}{b} \mapsto \tfrac{\sigma(a)}{\sigma(b)}\end{gathered}$$

任取 $\sigma \in S_n$, 则 σ 诱导出 n 元多项式环 $k[y_1, y_2, \cdots, y_n]$ 上的同构:

$$\begin{aligned}\tilde{\sigma} : k[y_1, y_2, \cdots, y_n] &\mapsto k[y_1, y_2, \cdots, y_n] \\ f(y_1, y_2, \cdots, y_n) &\mapsto f(y_{\sigma(1)}, y_{\sigma(n)}, \cdots, y_{\sigma(n)})\end{aligned}$$

从而 $\tilde{\sigma}$ 可以开拓为 $E = \mathrm{Frac}(k[y_1, y_2, \cdots, y_n])$ 的自同构 σ^*. 容易知, σ^* 保持 F 不动. 即 $\sigma^* \in \mathrm{Gal}(E/F)$. 于是, 我们定义映射:

$$\begin{gathered}\varphi : S_n \mapsto \mathrm{Gal}(E/F) \\ \sigma \mapsto \sigma^*\end{gathered}$$

φ 是单射. 于是 $|S_n| \leq |\mathrm{Gal}(E/F)|$. 于是 $|S_n| = |\mathrm{Gal}(E/F)|$, 故 $\mathrm{Gal}(E/F) \cong S_n$. 当 $n \geq 5$ 时, S_n 不可解, 由 Galois 理论, $f(x)$ 不可根式求解. □

到此, 我们完美的解决了 n 次一般方程的根式求解问题, 这是 Galois 理论的开端.

3.3.3 Galois 对应

随着人们的探索, Galois 理论的核心是 Galois 对应. 对于无限 Galois 扩域, 我们可以通过使用范畴论正向 (反向) 极限的语言, 及引入拓扑群推广 Galois 对应. 无限扩张的 Galois 群上引入拓扑结构, 是 Krull Topology 和绝对 Galois 群产生的原因之一. 在

两者的基础上, Galois 表示诞生, 它有着丰富的几何结构. 绝对 Galois 群为紧拓扑群, 它一般无法直接写出生成元及生成关系来了解结构, 借助表示论研究是自然的结果, 同时其在代数数论当中也有重要的作用. 考察范畴正向 (反向) 系统和极限, 投射有限群是重要的例子, 其是有限群论的重要研究对象.

首先, 我们引入" 可分" 的概念, 它不但有助于计算 Galois 群的阶数, 而且是了解 Galois 扩张的基本语言.

定义 3.3.30. 称域 k 上的不可约多项式 $p(x)$ 为**可分的** (separable), 如果它没有重根. 称域 k 上任意多项式 $f(x)$ 是**可分的**, 如果它的不可约因式都是可分的; 否则, 我们称为**不可分**多项式.

定义 3.3.31. E/k 为域扩张, 称 $\alpha \in E$ 为**可分元素** (separable element), 如果 α 是超越元或者 α 为代数元, 其在域 k 上的极小多项式 $\mathrm{Irr}(\alpha, k)$ 为可分多项式. 称域扩张 E/k 为**可分扩张** (separable), 若 $\forall \alpha \in E$, α 为可分元素; 否则称不可分扩张.

下面, 我们给出可分扩张的例子和性质:

例 3.3.32. (1) k 是一个域, 若 $\mathrm{Char}\, k = 0$, 则域 k 上的不可约多项式无重根. k 上的多项式都是可分多项式, E/k 任意域扩张都是可分扩张.

(2) 可分多项式的分裂域是可分扩张.

(3) E 是有限域, $|E| = p^n$, 其中 p 是素数. 若 $k \subseteq E$, E/k 为可分扩张. 因为 $\forall \alpha \in E$, $\mathrm{Irr}(\alpha, k) | (x^{p^n} - x)$, 而多项式 $(x^{p^n} - x)$ 在 E 上无重根.

下面, 我们给出一个定理, 它是 Galois 对应的开端. 在数学其他分支中, 类似于 Galois 对应的对应也广泛存在.

定理 3.3.33 (Galois 扩张等价定理). *E/k 为有限扩张, 域扩张的 Galois 群为 $G = \mathrm{Gal}(E/k)$. 以下等级:*

(1) E 是域 k 上某个可分多项式的分裂域.

(2) $k = E^G = \{a \in E \mid \forall \sigma \in \mathrm{Gal}(E/k), \sigma(a) = a\}$.

(3) $p(x) \in k[x]$ 为首一不可约多项式, 则 $p(x)$ 在 $E[x]$ 上是可分的, 且可唯一表示为一次因式的乘积.

证明. 参考 Rotman 英文原版书籍 *Advanced Algebra* Theroem A.5-42. Part I .Page. 206. □

定义 3.3.34. 称有限扩张 E/k 为 **Galois 扩张**, 如果它满足上述定理中的任何一条. 特别地, 在无限扩域下, 若域扩张 E/k 满足 $k = E^G$, 称 E/k 为 Galois 扩张. E/k 为 Galois 扩张, B 是中间域, 称 B 的**共轭** (conjugate) 为 $\sigma(B) = \{\sigma(b) : b \in B\}$, 其中 $\sigma \in \mathrm{Gal}(E/k)$.

关于 Galois 扩张, 我们有以下性质:

命题 1. E/k 是有限 Galois 扩张, 则:

(1) **(Galois 扩张的提升性)**: B 是中间域, 则 E/B 为 Galois 扩张.

(2) **(Galois 扩张中间域为 Galois 扩张的条件)**: B 是中间域, B/k 是 Galois 扩张, 当且仅当 B 的共轭为 B.

(3) **(Steinitz)** 有限扩张 E/k 是单扩张, 当且仅当它有有限个中间域. 有限 Galois 扩张仅有有限个中间域, 故有限 Galois 扩张是单扩张.

(4) 有限 Galois 扩张 E/k 的 Galois 群 $\mathrm{Gal}(E/k)$ 是 Abel 群, 则 E/k 的每个中间域 B/k 都是 Galois 扩张.

(5) **(Galois)**:k 是一个域, $\mathrm{Char}\, k = 0$, $f(x) \in k[x]$, E/k 是 Galois 扩张, 若 $G = \mathrm{Gal}(E/k)$ 是可解群, 则 E 可以嵌入到 k 的根式扩张中. 特别地, $f(x)$ 根式可解, 当且仅当 $f(x)$ 的 Galois 群是可解群.

证明. (1): 参考 Rotman 英文原版书籍 *Advanced Algebra* Corollary A.5-44. Part I .Page. 207.

(2): 参考 Rotman 英文原版书籍 *Advanced Algebra* Proposition A.5-45. Part I .Page. 207.

(3), (4): 参考 Rotman 英文原版书籍 *Advanced Algebra* Theroem A.5-53; Corollary A-5.54; Theorem 4.5-55 Part I .Page. 213—214.

(5): 参考 Rotman 英文原版书籍 *Advanced Algebra*Theroem A.5-62; Corollary A.5-63. Part I .Page. 207. □

下面, 我们给出 Galois 对应, 并且分别用格的语言和范畴的语言描述 Galois 对应.

定理 3.3.35 (Galois 对应基本定理). *E/k 是一个有限 Galois 扩张, $G = \mathrm{Gal}(E/k)$ 是其 Galois 群, 则我们有以下对应关系:*

(1) G 的子群 $\mathrm{Sub}(\mathrm{Gal}(E/k))$ 与 E/k 的中间域 $\mathrm{Int}(E/k)$ 之间存在一一对应的反序对应关系, 称之为 ***Galois* 对应**.

$$\begin{aligned} \gamma \quad & \mathrm{Sub}(\mathrm{Gal}(E/k)) \mapsto \mathrm{Int}(E/k) \\ & H \mapsto E^H \end{aligned}$$

$$\begin{aligned} \delta \quad & \mathrm{Int}(E/k) \mapsto \mathrm{Sub}(\mathrm{Gal}(E/k)) \\ & B \mapsto \mathrm{Gal}(E/B) \end{aligned}$$

其中, δ, γ 是**反序的** *(order—reversing)*. 即 $H_1 \le H_2 \le G$, $E^{H_2} \subseteq E^{H_1}$.

(2)

$$\forall B \in Int(E/k), \quad E^{\mathrm{Gal}(E/B)} = B$$

$$\forall H \in \mathrm{Sub}(\mathrm{Gal}(E/k)), \quad \mathrm{Gal}(E/E^H) = H$$

(3) ***Galois* 群和 *Galois* 扩张间的运算***:*

$$\forall H, K \in \mathrm{Sub}(\mathrm{Gal}(E/k)); A, B \in \mathrm{Int}(E/k)$$

$$E^{\langle H \cup K \rangle} = E^H \cap E^K$$

$$E^{H \cap K} = \langle E^H \cup E^K \rangle$$

$$\mathrm{Gal}(E/\langle A \cup B \rangle) = \mathrm{Gal}(E/A) \cap \mathrm{Gal}(E/B)$$

$$\mathrm{Gal}(E/A \cap B) = \langle \mathrm{Gal}(E/A) \cap \mathrm{Gal}(E/B) \rangle$$

(4) ***Galois* 群的指数和 *Galois* 扩张的次数***:*

$$\forall B \in \mathrm{Int}(E/k), [B : k] = [G : \mathrm{Gal}(E/B)]$$

$$\forall H \in \mathrm{Sub}(\mathrm{Gal}(E/k)), [G : H] = [E^H : k]$$

(5) $B \in \mathrm{Int}(E/k)$*,* B/k *是 Galois 扩张, 当且仅当* $\mathrm{Gal}(E/B) \triangleleft G$*.*

证明. 参考 Rotman 英文原版书籍 *Advanced Algebra*Theroem A.5-51; Part I .Page. 211—212. □

下面, 我们用格的语言来阐述 Galois 对应. 为此, 我们简单的介绍格.

定义 3.3.36. L 为偏虚集, 称 L 为一个**格** (lattice), 若 $\forall a, b \in L$, 在 L 中存在两者的下确界与上确界, 分别记为 $a \wedge b$, $a \vee b$. 称格 $L, L^{'}$ 同构, 若存在双射.

我们指出, Galois 对应中存在两个格.

例 3.3.37. 下面是格的例子.

(1) E/k 是域扩张, 则 $\mathrm{Int}(E/k)$ 关于子域自然关系形成一个偏序集 $(\mathrm{Int}(E/k), \leq)$. 其中, 任意两个中间域 A, B, 上确界为 $\langle A \cup B \rangle$, 下确界 $A \cap B$. 于是 $(\mathrm{Int}(E/k), \leq)$ 为一个格.

(2) G 是一个群, 则 $\mathrm{Sub}(G)$ 关于子群自然关系形成一个偏序集 $(\mathrm{Sub}(G), \leq)$. 其中, 任意两个子群 A, B, 上确界为 $\langle A \cup B \rangle$, 下确界 $A \cap B$. 于是 $(\mathrm{Sub}(G), \leq)$ 为一个格.

于是, 我们有 Galois 对应的格表示.

定理 3.3.38 (Galois 对应的格表示). *Galois 对应本质上是格* $\{\mathrm{Sub}(\mathrm{Gal}(E/k)), \leq\}$ *和格* $\{\mathrm{Int}(E/k), \leq\}$ *的反同构.*

定理 3.3.39 (Galois 对应的范畴表示). E/k *为有限 Galois 扩张,* $G = \mathrm{Gal}(E/k)$ *为 Galois 群.*

(a) $\mathfrak{f}(E/k)$ 是一个范畴, 其中对象为中间域 $k \subseteq B \subseteq E$, 态射为嵌入映射.

(b) $\mathfrak{g}(E/k)$ 是一个范畴, 其中对象为 *Galois* 群的子群 $H : H \leq \mathrm{Gal}(E/k)$, 态射为嵌入映射.

(c) $\mathrm{Gal} : \mathfrak{f}(E/k) \mapsto \mathfrak{g}(E/k)$ 是反变函子.

$$\begin{aligned} \mathrm{Gal} : \mathfrak{f}(E/k) &\mapsto \mathfrak{g}(E/k) \\ B &\mapsto \mathrm{Gal}(E/B) \end{aligned}$$

(d) $\mathrm{Inv} : \mathfrak{g}(E/k) \mapsto \mathfrak{f}(E/k)$ 是反变函子.

$$\begin{aligned} \mathrm{Inv} : \mathfrak{g}(E/k) &\mapsto \mathfrak{f}(E/k) \\ H &\mapsto \mathrm{Inv}(H) = E^H \end{aligned}$$

现在, 我们将上述 Galois 对应推广到无限次 Galois 扩张中. 为此, 我们需要借助拓扑群以及范畴论中极限的语言.

定义 3.3.40. 称群 G 为**拓扑群** (topological group), 若

1. G 为 Hausdorff 拓扑空间.

2. G 上的乘法和除法运算都是连续映射:

$$\begin{aligned} u : G \times G &\mapsto G \\ (u, v) &\mapsto uv \\ v : G &\mapsto G \\ x &\mapsto x^{-1} \end{aligned}$$

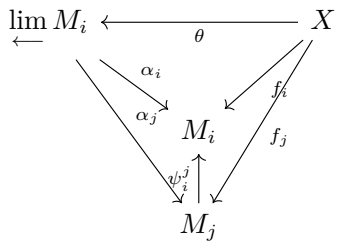
定义 3.3.41. $\mathcal{C}$ 是一个范畴, I 是一个偏序集, 偏序集 I 在范畴 $\mathcal{C}$ 上的**反向系统** (inverse system)$\{M_i; \psi_i^j\}$ 由一些对象 $(M_i)_{i\in I}$ 和态射 $\psi_i^j : M_j \mapsto M_i (i \preceq j)$ 构成, 使得如下图交换:

$$\begin{array}{ccc} M_k & \xrightarrow{\psi_i^k} & M_i \\ \downarrow{\scriptstyle \psi_j^k} & \nearrow{\scriptstyle \psi_i^j} & \\ M_j & & \end{array}$$

其中, $i \preceq j \preceq k$.

定义 3.3.42. I 为偏序集, $\mathcal{C}$ 为范畴, I 在范畴 $\mathcal{C}$ 上的反向系统为 $\{M_i; \psi_i^j\}_{i\in I}$. 称反向系统的**反向极限** (inverse limit) 为由一个对象 (记为 $\varprojlim M_i$) 及一簇态射 $\{\alpha_i : \varprojlim M_i \mapsto M_i\}_{i\in I}$ 构成的整体, 并且对任意的 $X \in \mathrm{Obj}(\mathcal{C}), f_i : X \mapsto M_i$, 存在唯一的态

射 $\theta : X \mapsto \varprojlim M_i$ 如下交换图成立:



性质 3.3.43. *I 是偏序集, R 是一个环, $\{M_i \mid \psi_i^j\}$ 为偏序集 I 上的左 $R-$ 模反向系统, 则其反向极限存在且唯一.*

证明. 参考 Rotman 英文原版书籍 *Advanced Algebra*Proposition B-7.2; Part I .Page. 653. □

对偶的, 我们还有**正向系统** (direct system) 和**正向极限** (direct limit) 的概念. 可参考参考 Rotman 英文原版书籍 *Advanced Algebra* Part I Page. 657—665.

性质 3.3.44. *下面是一些拓扑群的例子和性质.*

1. *G 为一个群, G 上赋予离散拓扑, 则 G 是一个拓扑群.*
2. *$(G_i)_{i\in I}$ 为拓扑群簇, 则 $\prod\limits_{i\in I} G_i$ 为拓扑群.*
3. *$\{G_i, \Psi_i^j\}$ 为一个逆向系统, 则逆向系统的反向极限 $\varprojlim\limits_{i\leftarrow I} G_i$ 是一个拓扑群.*
4. *E/k 是 Galois 扩张, 则 $\mathrm{Gal}(E/k)$ 为一个紧致拓扑群.*

下面, 我们给出无限次 Galois 扩张的 Galois 对应定理:

定理 3.3.45 (无限 Galois 对应). *E/k 是一个有限 Galois 扩张, $G = \mathrm{Gal}(E/k)$ 是其 Galois 群, 则我们有以下对应关系: G 的子群 $\mathrm{Sub}(\mathrm{Gal}(E/k))$ 与 E/k 的中间域 $\mathrm{Int}(E/k)$ 之间存在一一对应的反序对应关系, 称之为 **Galois 对应**.*

$$\begin{aligned} \gamma \quad & \mathrm{Sub}(\mathrm{Gal}(E/k)) \mapsto \mathrm{Int}(E/k) \\ & H \mapsto E^H \end{aligned}$$

$$\begin{aligned} \delta \quad & \mathrm{Int}(E/k) \mapsto \mathrm{Sub}(\mathrm{Gal}(E/k)) \\ & B \mapsto \mathrm{Gal}(E/B) \end{aligned}$$

*其中, δ, γ 是**反序的** (order—reversing). 即 $H_1 \le H_2 \le G$, $E^{H_2} \subseteq E^{H_1}$.*

注 41. 无限 Galois 对应, 格的描述和范畴的描述任然成立. 无限 Galois 对应建立了 Galois 扩张中间域与 Galois 群闭子群间的一一对应.

最后, 我们引出两个重要的概念, 它们在代数数论和 Galois 表示中有着重要作用.

定义 3.3.46. k 是一个域, 称 $\overline{k_s}$ 为 k 的**可分代数闭包** (separable algebraic closure), 若 $\overline{k_s}$ 为**极大可分扩张**: $S = \{\alpha \in \overline{k} \mid \alpha$为 k 上的可分元素$\}$. 称 $\mathrm{Gal}(\overline{k_s}/k)$ 为**绝对 Galois 群** (absolute Galois group).

3.3.4 低维 Galois 群的计算

Galois 群的计算是一个深刻的问题. 众所周知, 同调群的计算可由五大公理论解决: 维数公理, 函子公理, 正合公理, 同论公理, 切除公理 (等价于 Mayer—Viector 正合序列). 而对于 Galois 群的计算, 目前没有类似于同调群的计算机制. 借助可分性质和多项式的判别式, 我们已经解决了低维的 Galois 群计算问题 (三次和四次).

可分性质帮助我们计算 Galois 群的阶数, 是我们计算 Galois 群的有力工具. 低维 Galois 群的计算, 判别式 (discriminate) 是重要工具.

性质 3.3.47. *关于可分扩张计算 Galois 群的阶, 我们列出以下结论:*
(1) $\varphi : k \mapsto k'$ *为域同构,* φ *诱导出多项式环的同构:*

$$\begin{aligned} &\varphi^* : k[x] \mapsto k'[x] \\ &\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \varphi(a_i) x^n \end{aligned}$$

$f(x) \in k[x]$ *是可分多项式,* E/k *为* $f(x)$ *的分裂域,* E'/k' *是多项式* $\varphi^*(f(x))$ *的分裂域, 则存在* $[E : k]$ *个不同的* φ *的开拓:* $\Psi : E \mapsto E'$ *为同构.*

$$\begin{array}{ccc} E & \xrightarrow{\Psi} & E' \\ \uparrow & & \uparrow \\ k & \xrightarrow{\varphi} & k' \end{array}$$

(2) E/k *是* $f(x)$ *的分裂域,* $f(x)$ *为可分多项式, 则*

$$|\mathrm{Gal}(E/k)| = [E : k]$$

(3) $f(x) \in k[x]$ *为* n *次可分多项式,* E/k *为* $f(x)$ *的分裂域, 如果* $f(x)$ *是不可约多项式, 则*

$$n \mid |\mathrm{Gal}(E/k)|$$

(4) p *是一个素数,*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_{\ltimes} = \langle F_r \rangle$$

其中, $F_r : u \mapsto u^p$ *为* ***Frobenius* 自同构**.

(5) *Galois 多项式给出了判断多项式*$\mathbf{不可约的准则}$ *(irreducibility criterion):* $f(x)$ *不可约, 当且仅当* $\mathrm{Gal}(E/k)$ *传递地作用到* $f(x)$ *的根集. 即* $\forall \alpha, \beta \in E$ *均为* $f(x)$ *的根, 存在* $\sigma \in \mathrm{Gal}(E/k)$*, 使得* $\sigma(\alpha) = \beta$*.*

证明. (1), (2): 参考 Rotman 英文原版书籍 *Advanced Algebra* Theorem A-5.7; Part I .Page. 183.
(3): 参考 Rotman 英文原版书籍 *Advanced Algebra* Corollary A-5.9; Part I .Page. 184.
(4): 参考 Rotman 英文原版书籍 *Advanced Algebra* Theroem A-5.13; Part I .Page. 186.
(5): 参考 Rotman 英文原版书籍 *Advanced Algebra* Proposition A-5.14; Part I .Page. 187. □

定义 3.3.48. k 是一个域, $f(x) \in k[x]$ 为首一多项式. E/k 为 $f(x)$ 的分裂域, 则在 $E[x]$ 上有分解:

$$f(x) = \prod_i (x - \alpha_i)$$

其中, $\alpha_1, \alpha_2, \cdots, \alpha_n$ 为 $f(x)$ 的根. 定义:

$$\Delta = \Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)$$

称 $D = D(f) = \Delta^2 = \prod\limits_{i<j} (\alpha_i - \alpha_j)^2$ 为多项式的$\mathbf{判别式}$ (discriminate).

注 42. (1) $f(x)$ 有重根, 当且仅当 $D(f) = 0$.
(2) $\forall \sigma \in \mathrm{Gal}(E/k)$, σ 置换不同的根, 保持重根.
(3) $\forall \sigma\, \mathrm{Gal}(E/k)$,

$$\sigma(\Delta) = \prod_{i<j} (\sigma(\alpha_i) - \sigma(\alpha_j)) = \pm\Delta$$

故定义多项式的判别式为 $D = \Delta^2$ 是自然的, 因为 Δ 不仅依赖于 $f(x)$ 的根, 而且依赖于根的顺序.

性质 3.3.49. k *是一个域,* $f(x) \in k[x]$*, 若* $f(x)$ *是可分多项式, 则* $D(f) \in k$*.*

证明. 设 E/k 是 $f(x)$ 的分裂域, 因为 $f(x)$ 为可分多项式, 故 E/k 是 Galois 扩张, 从而 $E^{\mathrm{Gal}(E/k)} = k$. 任取 $\sigma \in \mathrm{Gal}(E/k)$, σ 置换 $f(x)$ 的根集. 于是,

$$\sigma(D) = \sigma(\Delta^2) = \sigma(\Delta)^2 = D$$

即 $D(f) \in E^{\mathrm{Gal}(E/k)} = k$. □

例 3.3.50. 下面, 我们给出一些低次多项式的判别式.

(1) 二次多项式: $f(x)=x^2+bx+c\in k[x]$, k 是一个特征不为 2 的域.

$$D(f)=\Delta^2=(\alpha-\beta)^2=b^2-4c$$

其中, α,β 为 $f(x)$ 的两个根.

(2) 三次多项式: $f(x)\in k[x]$, k 是一个域.

$$D(f)=\Delta^2=(\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$$

其中, α,β 为 $f(x)$ 的两个根.

下面, 我们阐述三次多项式的 Galois 群的计算结果.

定义 3.3.51. k 是一个域,

$$f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_0\in k[x]$$

对于 $\operatorname{Char}k=0$或者 $\operatorname{Char}k=p\nmid n$, 作变换 $x\mapsto x-\frac{1}{n}c_{n-1}$, 可得到 $f(x)$ 的**约化多项式** $\tilde{f}(x)$(reduced polynomial), 其不含 x^{n-1} 次项. 特别地, $\beta\in k$ 为 $f(x)$ 的约化多项式 $\tilde{f}(x)$ 的根, 当且仅当 $\beta-\frac{1}{n}c_{n-1}$ 为 $f(x)$ 的根.

首先, 我们给出三次多项式的判别式公式.

定理 3.3.52 (**三次首一多项式的判别式**)**.** *k 是一个域, $\operatorname{Char}k=0$, 则我们有:*

(1) $f(x)\in k[x]$, $\tilde{f}(x)$ 为其约化多项式, 则多项式的判别式等于其约化多项式的判别式.

$$D(f)=D(\tilde{f})$$

(2) $f(x)$ 是三次首一多项式, $\tilde{f}(x)=x^3+qx+r$ 为其约化多项式, 对于三次方程的约化多项式, 我们可计算其判别式:

$$D(f)=D(\tilde{f})=-4q^3-27r^2$$

证明. 参考 Rotman 英文原版书籍 *Advanced Algebra* Theroem A-5.68; Part I .Page. 224. □

注 43. 对于一般的 n 次方程, 我们可以通过**结式** (resultant) 进行计算. 设

$$f(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0\in k[x]$$

$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0\in k[x]$$

称 $f(x)$ 与 $g(x)$ 的结式为:

$$\operatorname{Res}(f,g)=\det(M)$$

其中, 矩阵 M 为 $(m+n)$ 的方阵:

$$M=\begin{bmatrix} a_m & a_{m-1} & \cdots a_1 & a_0 & \\ & a_m & \cdots & a_1 & a_0 \\ & & & & \\ b_n & b_{n-1} & \cdots b_1 & b_0 & \\ & b_n & \cdots & b_1 & b_0 \end{bmatrix}$$

$\mathrm{Res}(f,g)=0$ 当且仅当 f 和 g 有着非常值的公因子. 对于一般 n 次方程,

$$D(f)=(-1)^{\frac{n(n-1)}{2}}\mathrm{Res}(f,f')$$

其中, f' 是多项式 f 的形式微分.

下面, 我们可以用判别式计算多项式的 Galois 群.

定理 3.3.53 (**三次首一多项式的 Galois 群计算**). *$f(x)\in\mathbb{Q}[x]$ 为三次不可约多项式, G 是 $f(x)$ 的 Galois 群, D 为 $f(x)$ 的判别式, 则:*

(1) $f(x)$ 恰有一个实根, 当且仅当 $D<0$, $G\cong S_3$.

(2) $f(x)$ 有三个实数根, 当且仅当 $D>0$, 若 $\sqrt{D}\in\mathbb{Q}$, 则 $G\cong\mathbb{Z}_3$; 若 $\sqrt{D}\notin\mathbb{Q}$, 则 $G\cong S_3$

证明. 参考 Rotman 英文原版书籍 *Advanced Algebra* Proposition A-5.70; Part I .Page. 226. □

例 3.3.54. 三次多项式 Galois 群的计算例子:

(1) $f(x)=x^3-2\in\mathbb{Q}[x]$ 是不可约多项式, 通过计算判别式 $D=-108<0$, 于是 $f(x)$ 仅有一个实数根, 其 Galois 群 $\mathrm{Gal}(f)\cong S_3$, 从而 $f(x)$ 是根式可解的.

(2) $f(x)=x^3-4x+2\in\mathbb{Q}[x]$ 不可约多项式, 通过计算判别式 $D=108>0$, 且 $\sqrt{D}\notin\mathbb{Q}$ 于是 $f(x)$ 有三个实数根, 其 Galois 群 $\mathrm{Gal}(f)\cong S_3$, 从而 $f(x)$ 是根式可解的.

对于四次方程, 我们类似于三次方程判别式和约化多项式的使用技巧引入三次预解式.

定义 3.3.55. k 是一个域, $f(x)\in k[x]$. $\deg(f(x))=4$. 设 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 是 $f(x)$ 的根. 令

$$\begin{cases} u=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4) \\ v=(\alpha_1+\alpha_3)(\alpha_2+\alpha_4) \\ w=(\alpha_1+\alpha_4)(\alpha_2+\alpha_3) \end{cases}$$

任何特征为 0 或者 $\operatorname{Char} k = p \nmid n$ 域上的多项式. 我们可以转化为约化多项式. 再次, 称 $f(x) = x^4 + qx^2 + rx + s$ 的**三次预解式** (resolvement cubic) 为:

$$g(x) = (x-u)(x-v)(x-w)$$

通过计算, 我们得到 $f(x)$ 的三次预解式为:

$$g(x) = x^3 - 2q^2 + (q^2 - 4s)x + r^2$$

具体推导可参考 Rotman 英文原版书籍 *Advanced Algebra* Proposition A-5.74; Part I .Page. 230.

定理 3.3.56 (四次首一多项式的判别式). *$f(x) \in \mathbb{Q}[x]$ 的四次多项式, 则*

(1) $D(f) = D(g)$, 其中 g 是 f 的三次预解式.

(2) $f(x)$ 不可约, 则其三次预解多项式 g 无重根.

证明. 参考 Rotman 英文原版书籍 *Advanced Algebra* Proposition A-5.75; Part I .Page. 230—231. □

定理 3.3.57 (四次首一多项式的 Galois 群计算). *$f(x) \in \mathbb{Q}[x]$ 为四次不可约多项式, G 是 $f(x)$ 的 Galois 群, D 为 $f(x)$ 的判别式, $g(x)$ 是 $f(x)$ 的三次预解式, m 是 $g(x)$ 的 Galois 群的阶, 则:*

(1) 若 $m = 6$, 则三次预解式 $g(x)$ 在 $\mathbb{Q}[x]$ 上为不可约多项式, 若 $\sqrt{D}$ 为无理数, 则 $G \cong \mathbb{S}_4$.

(2) 若 $m = 3$, 则三次预解式 $g(x)$ 在 $\mathbb{Q}[x]$ 上为不可约多项式, 若 $\sqrt{D}$ 为有理数, 则 $G \cong \mathbb{A}_4$.

(3) 若 $m = 1$, 则三次预解式 $g(x)$ 在 $\mathbb{Q}[x]$ 上可完全分解,

$$G \cong \boldsymbol{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$$

(4) 若 $m = 2$, 则三次预解式 $g(x)$ 在 $\mathbb{Q}[x]$ 上有一个不可约的二次因式, $G \cong D_8$ 或者 $G \cong \mathbb{Z}_4$.

证明. 参考 Rotman 英文原版书籍 *Advanced Algebra* Proposition A-5.76; Part I .Page. 231. □

例 3.3.58. (1) $f(x) = x^4 - 4x + 2\mathbb{Q}[x]$, $g(x) = x^3 - 8x + 16$ 为三次预解式. 可得:

$$G \cong S_4$$

(2) $f(x)=x^4-10^2+1\mathbb{Q}[x]$, $g(x)=x^3+20x^2+96x=x(x+8)(x+12)$ 为三次预解式. 可得:

$$G\cong \mathbf{V}=\{(1),(12)(34),(13)(24),(14)(23)\}$$

最后, 我们以著名的 Galois 公开问题结束 Galois 理论的简介. **Galois 公开问题**: 什么样的有限群 G, 使得存在域扩张 $E/\mathbb{Q}$ 为 Galois 扩张, 满足 $G\cong \mathrm{Gal}(E/\mathbb{Q})$. 对于次问题, 已去得部分进展:

(1) Hilbert: S_n 是上述性质的 Galois 群.

(2) Shafererich: 可解群为上述性质的 Galois 群.

(3) 有限单群的分类定理: 绝大多数单群为上述性质的 Galois 群.

3.4 自由模与投射模 (二)

介绍自由模的定义与等价刻画, 介绍自由模的基, 介绍投射模的定义, 等价刻画与性质, 介绍 Schanuel 引理

定义 3.4.1. R-模 F 称为**自由 (free)R-模**, 如果 F 同构于若干个 R 复制的直和, 即存在指标集 I(可以无限) 使得:

$$F=\sum_{i\in I}R_i$$

其中对一切 i, $R_i=\langle b_i\rangle\cong R$. 我们称 $B=\{b_i:i\in I\}$ 为 F 的基.

自由 $\mathbb{Z}$-模是自由 Abel 群, 每个交换环看成它自身上的模时, 是自由 R-模, 域 k 上的向量空间 V 是一个自由 k-模.

定理 3.4.2 (自由模的泛性质). *设 F 是由子集 B 生成的 R-模, 则 F 是一个 (同构于) 以 B 为基的自由 R-模, 当且仅当对任意 R-模 M 和任意函数 $\gamma:B\to M$, 存在一个唯一的 R-映射 $g:F\to M$ 使得对一切 $b\in B, g(b)=\gamma(b)$.*

$$\begin{array}{ccc} F & & \\ \uparrow & \overset{g}{\searrow} & \\ B & \xrightarrow{\gamma} & M \end{array}$$

证明. 每个元素 $v\in F$ 有形如下式的唯一表达式:

$$v=\sum_{b\in B}r_b b$$

其中 $r_b\in R$ 且几乎一切 $r_b=0$. 定义:

$$\begin{aligned} g:F&\mapsto M\\ v&\mapsto g(v)=\sum_{b\in B}r_b\gamma(b)\end{aligned}$$

反之, 如果定义 $A_b = Rb$, 即以 $\{b\}$ 为基自由 R-模, 则这个条件表明 F 是 $\{A_b : b \leftarrow B\}$ 的余积. 更详细地说, 定义内射 a_b, 它把 $r_b b$ 映射到第 b 个坐标为 $r_b b$, 其他坐标为 0 的" 向量". 和任意余积一样, 存在唯一的映射 $\$theta : F \to M$ 使得 $\theta_{a_b}(b) = \gamma(b)$. 映射 θ 和 g 在基 B 的每个元素上一致, 因此 $\theta = g$ 根据命题有:

$$F \cong \sum_{b\in B} A_b = \sum_{b\in B} Rb$$

所以 F 同构于以 B 为基的自由 R-模. □

定义 3.4.3. 基中元素的个数称为 F 的**秩 (rank)**, 记为 $\mathrm{rank}(F)$.

定理 3.4.4 (交换环上自由模秩的完全不变性). *交换环上的自由模的基类似于线性空间的基, 是一组完全不变量.*

(1) 如果 R 是非零交换环, 则自由 R-模 F 的任意两个基有相同的基数, 即元素个数相同.

(2) 如果 R 是非零交换环, 则自由 R-模 F 和 F' 同构当且仅当 $\mathrm{rank}(F) = \mathrm{rank}(F')$.

证明. (1) 选取 R 中的极大理想 I. 如果 X 是自由 R-模 F 的一个基, 则陪集的集合 $\{v + IF : v \in X\}$ 是域 R/I 上的向量空间 F/IF 的一个基. 如果 Y 是 F 的另一个基, 则同样的论证给出 $\{u + IF : u \in Y\}$ 是 F/IF 的基. 但向量空间的任意两个基的基数相同, 于是得到 $|X| = |Y|$.

(2) 设 X 是 F 的基, X' 是 F' 的基, 并设 $\gamma : X \to X'$ 是双射. 把 γ 和包含映射 $X' \to F'$ 复合起来, 可以假定 $\gamma : X \to F'$, 于是存在扩张 γ 的唯一 R-映射 $\varphi : F \to F'$. 同样, 可以把 $\gamma^{-1} : X' \to X$ 看作函数 $X' \to F$, 并存在扩张 γ^{-1} 的唯一映射 $\psi : F' \to F$. 最后, $\psi\varphi$ 和 1_F 都扩张 1_X. 因此 $\psi\varphi = 1_F$. 同样, 另一个复合是 $1_{F'}$, 因此 $\varphi : F \to F'$ 是同构.

反之, 假定 $\varphi : F \to F'$ 是同构. 如果 $\{v_i : i \in I\}$ 是 F 的基, 则易知 $\{\varphi(v_i) : i \in I\}$ 是 F' 基, 因为自由模 F' 的任意两个基大小相同, 所以 $\mathrm{rank}(F') = \mathrm{rank}(F)$. □

定理 3.4.5 (投射分解基本定理). *每个 R-模 M 都是一个自由 R-模 F 的一个商.*

证明. 设 R 是 R 的 $|M|$ 个复制的直和, 并设 $\{x_m : m \in M\}$ 是 F 的基. 存在 R-映射 $g : F \to M$ 使得对一切 $m \in M$, $g(x_m) = m$. 显然 g 是满射, 于是 $F/\operatorname{Ker} g \cong M$ □

上面的命题可以用来构造具有指定性质的模.

定义 3.4.6. 设 $\chi = \{x_i : i \in I\}$ 是自由 R-模 F 的基, 并设 $\Re = \{\sum_i r_{ji} x_i : j \in J\}$ 是 F 的子集. 如果 K 是由 $\Re$ 生成的 F 的子模, 则我们说模 $M = F/K$ 具有**生成元 (generator)**χ 和**关系 (relation)**$\Re$. 称有序对 $(\chi|\Re)$ 是 M 的**表现 (presentation)**.

定理 3.4.7 (自由模是投射模). *如果 R 是交换环, F 是自由 R-模, 则对每个满射 $p : A \to A''$ 和每个 $h : F \to A''$, 存在同态 g 使得下图交换:*

$$\begin{array}{ccccc} F & & & & \\ \downarrow{\scriptstyle g} & \searrow{\scriptstyle h} & & & \\ A & \xrightarrow{p} & A'' & \longrightarrow & 0 \end{array}$$

证明. 设 $\{b_i : i \in I\}$ 是 F 的基. 因 p 是满射, 对一切 i 有 $a_i \in A$ 使得 $p(a_i) = h(b_i)$. 则存在 R-映射 $g : F \to A$ 使得对一切 i, $g(b_i) = a_i$. 由于 $pg(b_i) = p(a_i) = h(b_i)$, 则 pg 和 h 在基 $\{b_i : i \in I\}$ 上一致, 则 $pg = h$. □

定义 3.4.8. 称满足 $pg = h$ 的映射 $g : F \to A$ 为 h 的一个**提升 (lifting)**.

定义 3.4.9. 称模 P 是**投射 (projective)** 的, 如果对任意的满射 p 和任意的映射 h, 存在提升 g, 即存在映射 g 使得下图交换:

$$\begin{array}{ccccc} P & & & & \\ \downarrow{\scriptstyle g} & \searrow{\scriptstyle h} & & & \\ A & \xrightarrow{p} & A'' & \longrightarrow & 0 \end{array}$$

性质 3.4.10. *模 P 是投射的, 当且仅当 $\mathrm{Hom}_R(P, \quad)$ 是正合函子.*

由于 Hom 函子是左正合的, 即对任意模 P 把 $\mathrm{Hom}_R(P, \quad)$ 作用到正合列:

$$0 \longrightarrow A' \xrightarrow{i} A \xrightarrow{p} A''$$

我们可以得到如下正合列:

$$0 \longrightarrow \mathrm{Hom}_R(P, A') \xrightarrow{i^*} \mathrm{Hom}_R(P, A) \xrightarrow{p^*} \mathrm{Hom}_R(P, A'') \ .$$

证明. 如果 P 是投射模, 则给定 $h : P \to A''$ 存在提升 $g : P \to A$ 使得 $pg = h$. 于是, 如果 $h \in \mathrm{Hom}_R(P, A'')$, 则 $h = pg = p(g) \in \mathrm{Im}\, p^*$, 从而 p^* 是满射. 因此 $\mathrm{Hom}_R(P, \quad)$ 是正合函子.

关于逆命题, 假定 $\mathrm{Hom}_R(P, \quad)$ 是正合函子, 从而 p^* 是满射: 如果 $\mathrm{Hom}_R(P, A'')$ 则存在 $g \in \mathrm{Hom}_R(P, A)$ 使得 $h = p^*(g) = pg$. 这就是说, 给定 p 和 h, 存在提升 g 使得图交换; 即 P 是投射模. □

性质 3.4.11. *模 P 是投射模当且仅当每个短正合列*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} P \longrightarrow 0$$

是可裂正合列.

证明. 如果 P 是投射模, 则存在 $j : P \to B$ 使得下图交换;

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{j} & \downarrow{\scriptstyle 1_P} & & \\ B & \xrightarrow[p]{} & P & \longrightarrow & 0 \end{array}$$

反之, 假定每个以 P 结束的短正合列分裂, 考虑图:

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ B & \xrightarrow{p} & C & \longrightarrow & 0 \end{array}$$

其中 p 是满射. 现在形成拉回:

$$\begin{array}{ccccc} D & \underset{j}{\overset{\alpha}{\longleftrightarrow}} & P & & \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle f} & & \\ B & \xrightarrow{p} & C & \longrightarrow & 0 \end{array}$$

在拉回图中 p 的满射性给出 α 的满射性. 根据假设, 存在映射 $j : P \to D$ 使得 $aj = 1_P$. 定义 $g : P \to B$ 为 $g = \beta j$. 验证:

$$pg = p\beta j = f\alpha j = f1_P = f$$

则 P 是投射模. □

性质 3.4.12. *R-模 P 是投射的当且仅当 P 是一个自由 R-模的直和项.*

证明. 假定 P 是投射模. 每个模都是自由模的商. 于是存在自由模 F 和满射 $g : F \to P$, 从而存在正合列

$$0 \longrightarrow \operatorname{Ker} g \longrightarrow F \xrightarrow{g} P \longrightarrow 0$$

表明 P 是 F 的直和项. 假设 P 是自由模 F 的直和项, 从而存在映射 $q : F \to P$ 和 $j : P \to F$ 满足 $qj = 1_p$. 现在考虑图:

$$\begin{array}{ccccc} F & \underset{j}{\overset{q}{\longleftrightarrow}} & P & & \\ \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle f} & & \\ B & \xrightarrow{p} & C & \longrightarrow & 0 \end{array}$$

其中 p 是满射. 复合 fq 是映射 $F \to C$; 由于 F 是自由的, 它必是投射的, 从而存在映射 $h : F \to B$ 满足 $ph = fq$. 定义 $g : P \to B$ 为 $g = hj$. 剩下要证明 $pg = f$. 但注意到:

$$pg = phj = fqj = f1_P = f.$$

□

例 3.4.13. 环 $R = I_6$ 是两个理想的直和:

$$I_6 = I \oplus J$$

其中:

$$J = \{[0], [2], [4]\} \cong I_3 \; I = \{[0], [3]\} \cong I_2$$

现在 I_6 是它自身上的自由模, 从而 I 和 J 作为自由模的直和项是投射 I_6-模. 然而, J 和 I 都不可能是自由的. 毕竟一个 (有限生成) 自由 I_6-模 F 是若干个 I_6 的复制的直和, 从而 F 有 6^n 个元素. 所以 J 太小而不能成为自由模, 因为它只有三个元素.

定理 3.4.14 (投射基的存在性). *R-模 A 是投射模, 当且仅当存在元素 $\{a_i : i \in I\} \subseteq A$ 和 R-映射 $\{\varphi_i : A \to R, i \in I\}$ 满足:*
(1) 对每个 $x \in A$, 几乎一切 $\varphi_i(x) = 0$;
(2) 对每个 $x \in A$, 有 $x = \sum_{i \in I}(\varphi_i x)a_i$.
此外, 在这种情形中 $\{a_i : i \in I\} \subseteq A$ 生成 A.

证明. 如果 A 是投射模, 则存在自由 R-模 F 和满射 R-映射 $\psi : F \to A$. 因 A 是投射的, 存在 R-映射 $\varphi : A \to F$ 使得 $\psi\varphi = 1_A$. 设 $\{e_i : i \in I\}$ 是 F 的基, 定义 $a_i = \psi(e_i)$. 现在, 如果 $x \in A$, 则存在唯一表达式 $\varphi(x) = \sum_i r_i e_i$, 其中 $r_i \in R$ 且几乎一切 $r_i = 0$. 定义 $\varphi_i : A \to R$ 为 $\varphi_i(x) = r_i$. 当然, 给定 x, 对几乎一切 i 有 $\varphi_i(x) = 0$. 因 ψ 是满射, 由 $\{a_i = \psi(e_i) : i \in I\}$ 生成. 最后,

$$x = \psi\varphi(x) = \psi\left(\sum r_i e_i\right) = \sum r_i \psi(e_i) = \sum(\varphi_i x)\psi(e_i) = \sum(\varphi_i x)a_i.$$

反之, 如命题陈述中给定 $\{a_i : i \in I\} \subseteq A$ 和一族 R-映射 $\{\varphi_i : A \to R, i \in I\}$, 定义 F 是以 $\{e_i : i \in I\}$ 为基的自由 R-模, 定义 R-映射 $\psi : F \to A$ 为 $\psi : e_i \mapsto a_i$. 现在只需找到一个 R-映射 $\varphi : A \to F$ 使得 $\psi\varphi = 1_A$, 因为由此可推出 A 是 F 的直和项, 因此 A 是投射模. 定义 φ 为 $\varphi(x) = \sum_i(\varphi_i x)e_i$, 其中 $x \in A$. 根据条件, 这个和是有限的, 从而 φ 是合理定义的. 由于,

$$\psi\varphi(x) = \psi\sum(\varphi_i x)e_i = \sum(\varphi_i x)\psi(e_i) = \sum(\varphi_i x)a_i = x;$$

即 $\psi\varphi = 1_A$ □

定义 3.4.15. 如果 A 是 R-模, 则满足上述命题中的条件的子集 $\{a_i : i \in I\} \subseteq A$ 和一族 R-映射 $\{\varphi_i : A \to R, i \in I\}$ 叫做**投射基 (projective basis)**.

定义 3.4.16. 称 R-模是**有限表现的 (finitely presented)**, 如果它有表现 $(\chi|\Re)$, 其中 χ 和 $\Re$ 都是有限的.

定理 3.4.17. *如果是交换 Noether 环, 则每个有限生成 R-模都是有限表现的.*

定理 3.4.18 (Schanuel 引理). *给定正合列:*

$$0 \longrightarrow K \xrightarrow{i} P \xrightarrow{\pi} M \longrightarrow 0$$

和

$$0 \longrightarrow K' \xrightarrow{i'} P' \xrightarrow{\pi'} M \longrightarrow 0$$

其中 P 和 P' 是投射模, 则存在同构:

$$K \oplus P' \cong K' \oplus P$$

证明. 考虑行正合的图

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & P & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & K' & \xrightarrow{i'} & P' & \xrightarrow{\pi} & M & \longrightarrow & 0 \end{array}$$

因 P 是投射的, 存在映射 $\beta : P \to P'$ 使得 $\pi'\beta = \pi$; 即图中右边的正方形交换, 我们现在证明存在映射 $\alpha : K \to K'$ 使得其他正方形交换. 如果 $x \in K$, 则因 $\pi i = 0$ 有 $\pi'\beta ix = \pi ix = 0$. 因此 $\beta ix \in \operatorname{Ker}\pi' = \operatorname{Im} i'$, 于是存在 $x' \in K'$ 使得 $i'x' = \beta ix$; 此外, 因 i' 是单射, 从而 x' 唯一. 所以 $\alpha : x \mapsto x'$ 是良定义的函数 $\alpha : K \to K'$, 它使得第一个正方形交换. 可证明 α 是 R-映射.

这个有两个正合行的交换图给出一个正合列:

$$0 \longrightarrow K \xrightarrow{\theta} P \oplus K' \xrightarrow{\psi} P' \longrightarrow 0 \ ,$$

其中 $\theta : x \mapsto (ix, ax)$ 和 $\psi : (u, x') \mapsto \beta u - i'x'$, 其中 $x \in K$, $u \in P$, $x' \in K'$. 可验证这个序列的正合性. 由于 P' 是投射模, 这个序列是分裂的. □

性质 3.4.19. *如果 M 是有限表现的且*

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

是正合列, 其中 F 是有限生成自由模, 则 K 是有限生成的.

证明. 因 M 是有限表现的, 存在正合列:

$$0 \longrightarrow K' \longrightarrow F' \longrightarrow M \longrightarrow 0$$

其中 F' 是自由的, F' 和 K' 都是有限生成的. 根据 Schanuel 引理(3.4.18), $K \oplus F' \cong K' \oplus F$. 现在, 因为 $K' \oplus F$ 的两个直和项都是有限生成的, 所以 $K' \cong F$ 是有限生成的, 从而左端也是有限生成的. 而直和项 K 是 $K \cong F'$ 的同态像, 因此它是有限生成的. □

3.5 内射模

在介绍了投射模之后, 我们进一步介绍其对偶概念内射模. 介绍内射模的定义, 内射模的等价刻画与性质, 并从所学的半单模和诺特环角度进一步探究内射模和它们的关系. 最后, 初步介绍有限 Abel 群的基定理.

定义 3.5.1. 如果 E 是 $R-$ 模, 如果反变函子 $\mathrm{Hom}_R(\quad, E)$ 是正合函子, 即 $\mathrm{Hom}_R(\quad, E)$ 保持一切 R-模的短正合列, 则称 E 为**内射模 (injective module)**.

注 44. 用图来刻画时, 内射模是投射模的对偶图. 内射模的图就是反转投射模图的一切箭头.

性质 3.5.2. *模 E 是内射模, 当且仅当只要 i 是单射, 则存在一个 f 的提升 g, 使得下图交换:*

$$\begin{array}{ccccc} & & E & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle g} & \\ 0 & \longrightarrow & A & \xrightarrow{i} & B \end{array}$$

即一个子模到 E 中的每个同态都可扩张为从一个大的模到 E 中的同态.

证明. 因 $\mathrm{Hom}_R(\ , E)$ 是左正合反变函子, 所以证明的关键为是只要 i 为单射, 则 i^{**} 是满射. 即根据正合列:

$$0 \longrightarrow A \xrightarrow{i} B$$

可得正合列:

$$\mathrm{Hom}_R(B, E) \xrightarrow{i^*} \mathrm{Hom}_R(A, E) \longrightarrow 0$$

(1) (必要性:) 如果 E 是内射模, 则 $\mathrm{Hom}(\ , E)$ 是正合函子, 故 i^* 是满射. 所以如果 $f \in \mathrm{Hom}_R(A, E)$, 则存在 $g \in \mathrm{Hom}_R(B, E)$, 使

$$f = i^* g = gi,$$

即图是交换的.

(2) (充分性:) 如果 E 满足图条件, 则给定 $f : A \to E$, 存在 $g : B \to E$, 使得 $gi = f$. 从而如果 $f \in \mathrm{Hom}_R(A, E)$, 则我们有:

$$f = gi = i^*(g) \in \mathrm{Im}(i^*)$$

故 i^* 是满射. 所以 $\mathrm{Hom}(\ , E)$ 是正合函子, E 为内射模.

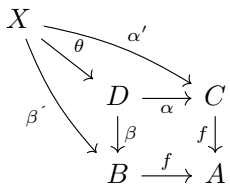
□

下面介绍两个概念用于下面的证明:

定义 3.5.3. 在范畴 $\mathcal{C}$ 中给定两个态射 $f : B \to A$ 和 $g : C \to A$, 一个**泛映射问题的解 (solution of universal mapping problem)** 是指有序三元组 (D, α, β) 使下图交换:

$$\begin{array}{ccc} D & \xrightarrow{\alpha} & C \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle g} \\ B & \xrightarrow{f} & A \end{array}$$

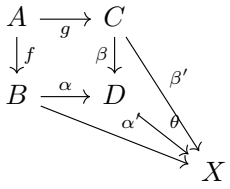
一个**拉回 (pull back)** 是指一个上述问题的最优解. 对于每个解 (X, α', β'), 存在唯一的态射 $\theta : X \to D$, 使下图交换:



定义 3.5.4. 对偶地, 有推出的概念在范畴 $\mathcal{C}$ 中给定两个态射 $f : A \to B$ 和 $g : A \to C$, 一个解是指有序三元组 (D, α, β) 使得下图交换:

$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \beta} \\ B & \xrightarrow{\alpha} & D \end{array}$$

一个**推出 (push out)** 是指一种最优解: 对每个解 (X, α', β'), 存在唯一的态射 $\theta : D \to X$ 使下图交换:



性质 3.5.5. 模 E 是内射模当且仅当每个短正合列

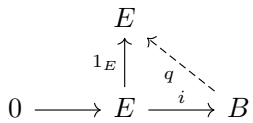
$$0 \longrightarrow E \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

都是分裂的.

证明. 如果 E 是内射模, 则存在

$$q : B \to E$$

使下图交换:



即 $qi = 1_E$. 由可裂正合列的等价刻画

$$0 \longrightarrow E \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

分裂. 反之, 假定每个以 E 开始的正合列分裂, 则:

$$\begin{array}{ccccc} & & E & & \\ & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & B \end{array}$$

的推出是

$$\begin{array}{ccccc} & & E & \xrightarrow{\alpha} & D \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle \beta} \\ 0 & \longrightarrow & A & \xrightarrow{i} & B \end{array}$$

由推出的性质知 α 是单射, 从而

$$0 \longrightarrow E \longrightarrow D \longrightarrow \operatorname{Coker}\alpha \longrightarrow 0$$

分裂. 即存在 $q : D \longrightarrow E$, 使 $q\alpha = 1_E$. 令 $g : B \longrightarrow E$, 其中 $g = q\beta$. 于是:

$$gi = q\beta i = q\alpha f = 1_E f = f$$

即图交换, 从而 E 为内射模. □

性质 3.5.6. 内射模的直和项是内射的.

证明. 设 S 是内射模 E 的直和项, 则有态射 $q : E \longrightarrow S$, $i : S \longrightarrow E$, 满足 $qi = 1_S$. 考虑图

$$\begin{array}{ccccc} & & S & \underset{q}{\overset{i}{\longleftrightarrow}} & E \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle g} & \uparrow{\scriptstyle h} \\ 0 & \longrightarrow & A & \xrightarrow{j} & B \end{array}$$

其中 j 是单射, i, f 是 $A \to E$ 的态射. 因 E 是内射模, 故存在态射 $h : B \longrightarrow E$, 使得 $hj = if$. 令 $g : B \longrightarrow S$, 使得 $g = qh$, 则有:

$$gj = qhj = qif = 1_S f = f,$$

故 S 是内射模. □

性质 3.5.7. 如果 $\{E_i : i \in I\}$ 是一族模, 则 $\prod_{i\in I} E_i$ 是内射模当且仅当每个 E_i 是内射模.

证明. (必要性:) 考虑图

$$\begin{array}{ccccc} & & E & & \\ & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & A & \xrightarrow{k} & B \end{array}$$

其中 $E = \pi E_i$, 且 $k : A \longrightarrow B$ 为单射. 令 $P_i : E \longrightarrow E_i$ 为第 i 个投影, 因 E_i 是内射模, 从而存在 $g_i : B \longrightarrow E_i$, 使得 $g_i k = p_i f$. 令

$$\begin{aligned} g : B &\longrightarrow E \\ b &\longrightarrow (g_i(b)) \end{aligned}$$

如果 $b = ka$, 则有:

$$g(ka) = (g_i(ka)) = (p_i(fa)) = fa$$

故 E 是内射模. (充分性:)

$$\prod_{k\in I} E_k = E_i \bigoplus \prod_{j\neq i} E_j$$

由性质(3.5)可得. □

定理 3.5.8 (Baer 判别法). *R-模 E 是内射模, 当且仅当每个 R-映射 $f : I \to E$ 都可以扩张到 R 上, 其中 I 是 R 中的理想. 即有交换图:*

$$\begin{array}{ccccc} & & E & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle g} & \\ 0 & \longrightarrow & I & \xrightarrow{i} & R \end{array}$$

证明. (必要性:) 因任一理想 I 都是 R 的子模, 所以 f 的一个扩张 g 的存在性正是 E 的内射性定义的特殊情形. (充分性:) 设有交换图:

$$\begin{array}{ccccc} & & E & & \\ & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & B \end{array}$$

其中, A 是 B 的子模. 假定 i 是包含映射. 设 X 是一切有序对 (A', g') 的集合, 其中 $A \subseteq A' \subseteq B$, $g' : A' \longrightarrow E$ 是 f 的扩张. 即 $g'|A = f$. 因 $(A, f) \in X$, 故 $X \neq \phi$. 现定义 X 上的偏序:

$$(A', g') \preceq (A'', g'')$$

其中, $A' \subseteq A''$; g'' 扩张 g'. 由 Zorn 引理, X 中存在极大元, 记为 (A_0, g_0). 如果 $A_0 = B$, 则结论已经证明, 否则可假设有 $b \in B, b \notin A_0$. 定义:

$$I = \{r \in R : rb \in A_0\},$$

可以证明 I 为 R 的理想. 定义:

$$h : I \longrightarrow E$$
$$r \longmapsto g_0(rb)$$

由假设, 存在 $h^* : R \longrightarrow E$ 扩张 h. 令 $A_1 = A_0 + \langle b \rangle$, 构造态射:

$$g_1 : A_1 \to E$$
$$a_0 + rb \mapsto g(a_0) + rh^*(1)$$

其中 $a_0 \in A_0, r \in R$. 下面, 我们需要证明 g_1 是良定义的. 如果 $a_0 + rb = a_0' + r'b$, 则:

$$(r - r')b = a_0' - a_0 \in A_0,$$

由此 $r - r' \in I$. 故 $g_0((r - r')b)$ 与 $h(r - r')$ 有定义, 且:

$$g_0(a_0' - a_0) = g_0((r - r')b) = h(r - r') = h^*(r - r') = (r - r')h^*(1).$$

由 $R-$ 映射的假设,

$$g_0(a_0') - g_0(a_0) = rh^*(1) - r'h^*(1),$$

故

$$g_0(a_0') + r'h^*(1) = g_0(a_0) + rh^*(1).$$

显然对一切 $a_0 \in A_0$, $g_1(a_0) = g_0(a_0)$, 故映射 g_1 扩张 g_0. 从而 $(A_0, g_0) \prec (A_1, g_1)$ 与 (A_0, g_0) 的极大性矛盾. 所以 $A_0 = B$, g_0 是 f 的提升, 故 E 是内射模. □

性质 3.5.9. *如果 R 是一个整环, 设 $Q = \mathrm{Frac}(R)$ 则有:*

(1) 如果 $f : I \to Q$ 是 R-映射, I 是 R 的理想, 则存在 $c \in Q$ 使得对于任意的 $a \in R$, 满足 $f(a) = ca$.

(2) Q 是内射 R-模.

(3) 如果 $g : Q \to Q$ 是 R-映射, 则存在 $c \in Q$, 使得对于任意的 $x \in Q$, $g(x) = cx$.

证明. (1) 如果 $a, b \in I$ 都不为 0, 则 $f(ab)$ 有定义, 且因为 f 为 $R-$ 映射得:

$$af(b) = f(ab) = bf(a),$$

因此 $\frac{f(a)}{a} = \frac{f(b)}{b}$. 令 $c = \frac{f(a)}{a}$, 则对于任意的 $a \in I$, $f(a) = ca$.

(2) 由 Baer 判别法(3.5.8), 只需证明对 R 的任意理想 I, $R-$ 映射 $f : I \longrightarrow Q$ 扩张到整个 R. 根据性质 (1), 存在 $c \in Q$, 使得对任意的 $a \in I$, $f(a) = ca$. 定义:

$$g : R \to Q$$
$$r \mapsto cr$$

容易看出, g 是扩张 f 的 $R-$ 映射, 故 Q 是内射模.

(3) 设 $g : Q \longrightarrow Q$ 是一个 $R-$ 映射, 令 $f = g|R : R \longrightarrow Q$. 由 (1) 中令 $I = R$ 得, 存在 $c \in Q$, 使得对于任意的 $a \in R$, 成立:

$$f(a) = g(a) = ca.$$

设 $x \in Q$, $x = \frac{a}{b}$, 其中 $a, b \in R$. 于是, $bx = a$; $g(bx) = g(a)$. 而 $g(bx) = bg(x)$, 故:

$$g(x) = (ca)/b = cx.$$

□

定义 3.5.10. 如果 R 是整环, 称一个 R-模 D 是**可除的 (divisible)**, 如果对每个 $d \in D$ 和每个非零 $r \in R$, 存在 $d' \in D$ 使 $d = rd'$.

例 3.5.11. 设 R 是整环, 则

(1) $\mathrm{Frac}(R)$ 是可除 R-模.

(2) 可除 R-模的每个直和都是可除的, 因此 $\mathrm{Frac}(R)$ 上的每个向量空间是可除 R-模.

(3) 每个可除 R-模的商是可除的.

引理 3.5.12. *如果 R 是整环, 则每个内射 R-模 E 都是可除的.*

证明. 设 E 是内射模, 设 $e \in E, r_0 \in R$ 为非 0 元素, 依定义, 要求出 $x \in E$, 使 $e = r_0 x$. 令

$$f : (r_0) \to E,$$

$$rr_0 \mapsto re$$

因 R 是整环, 由 $rr_0 = r'r_0$ 可知 $r = r'$. 故上述映射定义合理, 且显然为 $R-$ 映射. 因 E 是内射模, 存在 $h : R \to E$ 扩张 f. 则满足:

$$e = f(r_0) = h(r_0) = r_0 h(1),$$

因此 $x = h(1)$ 即为所求. □

推论 3.5.13. *设 R 是 PID, 则 R-模 E 是内射模当且仅当它是可除模.*

证明. 必要性, 根据引理(3.5.12)立得. 下证充分性: 设 E 是可除的, 由 Baer 判别法(3.5.8), 只需把 $R-$ 映射 $f : I \longrightarrow E$ 扩充到 R 上. 因 R 是 PID, 故 I 为主理想. 设 $I = (r_0)$, 其中 $r_0 \in I$. 因 E 是可除的, 故存在 $e \in E$, 使 $r_0 e = f(r_0)$. 令

$$h : R \to E$$

$$r \mapsto re$$

易知 h 是扩张 f 的 $R-$ 映射, 故 E 是内射模. □

注 45. 存在可除模不是内射模的整环. 事实上, 若 R 是一个整环但不是 Dedekind 环, 则存在非内射的 R-模是可除模.

例 3.5.14. 下面的 Abel 群都是内射 $\mathbb{Z}$-模:

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}/\mathbb{Z}, \mathbb{R}/\mathbb{Z}, \mathbb{S}$$

其中, $\mathbb{S}$ 是圆盘, $|z|=1$ 的一切复数 z 的乘法群.

推论 3.5.15. *每个 Abel 群 M 可以作为子群嵌入某个内射 Abel 群.*

证明. 我们已经知道每个 $R-$ 模 M 都是一个自由 $R-$ 模 F 的一个商. 此外, M 是有限生成的, 当且仅当 F 可以选取为有限生成的. 从而存在自由 Abel 群 $F=\sum_i Z_i$, 使得对某个 $K \subseteq F$ 有 $M = F/K$. 从而:

$$M = F/K = \left(\sum_i Z_i\right)/K \subseteq \left(\sum_i Q_i\right)/K.$$

根据例(3.5.11), Q_i 是可除模. 故 $\sum_i Q_i$ 可除. 所以 $(\sum_i Q_i)/K$ 是可除模, 故 $(\sum_i Q_i)/K$ 是内射模. □

注 46. 把一个模写作自由模的商模, 本质上是用生成元和关系描述(3.4.5).

定理 3.5.16 (内射分解基本定理). *对每个环 R, 任意左 R-模 M 可以作为子模嵌入某个内射左 R-模.*

证明. 将 M 先看作一个 Abel 群, 由推论(3.5.15)的证明, 存在一个可除的 Abel 群 D 和单 $\mathbb{Z}-$ 态射 $j: M \to D$. 固定一个 $m \in M$, 有 $f_m : r \mapsto j(rm)$. 其中, $f \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$. 令 $\varphi : m \mapsto f_m$, 则 φ 是一个单的 $R-$ 映射, 从 M 到 $\mathrm{Hom}_{\mathbb{Z}}(R, D)$, 而 $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ 是左内射模, 即得证. □

注 47. 存在包含任意给定模的最小内射模, 称为**内射包络 (injective envelope)**.

定理 3.5.17 (半单环的等价刻画). *R 是一个环, 则下列条件等价:*

(1) R 是半单的.

(2) 每个左/右 R-模是半单模.

(3) 每个左/右 R-模是内射的.

(4) 每个左/右 R-模短正合列是分裂的.

(5) 每个左/右 R-模是投射的.

证明. (A) (1) $\Longrightarrow$ (2) 因 R 是半单的, 故其正则模 $({}_RR)$ 是半单模. 因此, 每个自由 $R-$ 模是半单模. 根据性质(3.4.5), M 是自由模的商, 而自由 $R-$ 模是半单的, 故 M 是半单的.

(B) (2) $\Longrightarrow$ (3) 设 M 是左 $R-$ 模, 则 M 是内射模可由如下正合列是分裂正合列得到:

$$0 \longrightarrow M \longrightarrow B \longrightarrow C \longrightarrow 0$$

而 B 是半单模, M 可看作 B 的子模, $C = B/M$. 由半单性可知 $B = M \oplus M', C \cong B/M \cong M'$. 所以 $B \cong C \oplus M$, 正合列分裂.

(C) (3) $\Longrightarrow$ (4) 如果

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

是正合列, 只要 A 是内射模, 正合列分裂.

(D) (4) $\Longrightarrow$ (5) 给定模 M, 存在正合列

$$0 \longrightarrow F' \longrightarrow F \longrightarrow M \longrightarrow 0$$

M 是自由模的商模, 可令 F 为自由模. 由分裂性:

$$F \cong M \oplus F',$$

故 M 是自由模的直和项, 从而根据性质(3.4.12)知 M 为投射模.

(E) (5) $\Longrightarrow$ (1) 设 I 是 R 的左理想, 则:

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

由假设, R/I 投射, 故正合列是分裂的. 从而 I 是 R 的直和项, 即 R 的任一子模为直和项. 故 R 正则模半单, R 为左半单环.

□

注 48. 由于半单环上的模有优良性质, 我们希望测量 R 离开半单性的程度, 整体维数 (global dimension) 是测量环偏离半单性程度的重要工具.

性质 3.5.18. *(1) 如果 R 是 Noether 环, $\{E_i : i \in I\}$ 是一族内射 R-模, 则 $\sum_{i\in I} E_i$ 是内射模.*

*(2) (**Bass-Papp**) 如果 R 是环, 对于它每个内射左 R-模的直和也是内射模, 则 R 是左 Noether 环.*

证明. (1) 由 Baer 判别法(3.5.8), 只需完成如下交换图:

$$\begin{array}{ccccc} & & \sum_{i\in I} E_i & & \\ & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & J & \xrightarrow{k} & R \end{array}$$

其中 J 是 R 中理想, 因 R 是诺特环, 故 J 是有限生成的. 设

$$J = (a_1, \cdots, a_n),$$

其中, $f(a_k) \in \sum_{i\in I}$ 只有有限个非零坐标. 设它们出现在指标集 $S(a_k) \subseteq I$ 中. 于是 $S = \bigcup_{k=1}^{n} S(a_k)$ 是有限集. 从而 $\mathrm{Im}(f) \subseteq \sum\limits_{i\in S} E_i$. 故 $\sum\limits_{i\in S} E_i$ 为内射模, 此时存在 $R-$ 映射

$$g' : R \longrightarrow \sum_{i\in S} E_i$$

g' 扩张 f, 它是将 g' 和 $\sum_{i\in S} E_i$ 到 $\sum_{i\in I} E_i$ 的包含映射复合得到的.

(2) 设 R 不是左诺特环, 则存在左理想严格升链 $I_1 \subsetneq I_2 \subsetneq \cdots$. 令 $I = \cup I_n$, 且对于任意的 n, $I/I_n \neq 0$. 可以将 I/I_n 嵌入一个内射左 $R-$ 模 E_n. 断言, $E = \sum\limits_{n\in\mathbb{N}} E_n$ 不是内射模. 设 $\pi_n : I \to I/I_n$ 是自然映射, 对每个 $a \in I$ 对每个足够大的 n, $a \in I_n$. 故 $\pi_n(a) = 0$. 令

$$f : I \to \pi(I/I_n)$$

$$a \mapsto (\pi_n(a))$$

f 为 $R-$ 映射, 则其像在 $\sum\limits_{n\in\mathbb{N}}(I/I_n)$ 中, 即对 $a \in I, f(a)$ 的一切坐标几乎都等于零. 把 f 与包含映射结合:

$$i : \sum(I/I_n) \to \sum E_n = E$$

将 f 看作映射 $I \to E$. 如果存在扩张 f 的 $R-$ 映射 $g : R \to E$, 则 $g(1)$ 有定义. 设 $g(1) = (x_n)$. 选取一个指标 m, 选取 $a \in I, a \in I_m$, 则 $\pi_m(a) \neq 0$. 所以, $g(a) = f(a)$ 的第 m 个坐标 $\pi_m(a) \neq 0$. 而 $g(a) = ag(1) = a(x_n) = (ax_n)$, 所以 $\pi_m(a) = ax_m$. 故对于任意的 m, $x_m \neq 0$. 这与 $g(1)$ 在直和 $E = \sum E_n$ 中矛盾.

□

定理 3.5.19 (PID 商环上的正则模是内射模). *设 R 是 PID, $a \in R$ 既不是零也不是单位, 设 $J = (a)$, 则 R/J 是内射 R/J-模.*

证明. 由模同构的对应定理(1.3.16), R/J 中的每个理想形如 I/J, 其中 I 是 R 中包含 J 的某个理想. 设 $I = (b)$, 故 I/J 是循环的, 其有生成元 $x = b + J$. 因 $(a) \subseteq (b)$, 故存在 $r \in R$, 使得 $a = rb$. 设 $f : I/J \longrightarrow R/J$ 是 $R/J-$ 映射, 其中:

$$f : I/J \to R/J$$

$$b + J \mapsto f(b + J) = s + J$$

因为 $r(b + J) = rb + J = a + J = 0$, 且 $rf(b + J) = r(s + J) = rs + J = 0$, 故 $rs \in J = (a)$. 于是, 存在 $r' \in R$, 使得 $rs = r'a = r'br$. 故 $s = r'b$. 所以:

$$f(b + J) = s + J = r'b + J.$$

定义:

$$f : h : R/J \to R/J$$
$$u + J \mapsto r'u + J$$

于是我们有 $h(b + J) = f(b + J)$. 从而 h 扩张 f, 故 R/J 是内射模. □

推论 3.5.20 (Basis Theorem). *如果 R 是 PID, 则每个有限生成模 M 都是循环模的直和.*

第四章　高等线性代数

4.1　有限生成 Abel 群上的基定理

我们对线性空间的理论已非常熟悉, 前面谈到的自由模及其特例, 自由 Abel 群, 它们的结构和线性空间类似. 但对于自由模, 一个可能会忽视的点是有可能 $rm = 0$, $r \neq 0$, $m = 0$ 成立. 即跟一般的线性空间的性质有一定差别. 本节就是专门讨论自由模不同于线性空间的特殊性质, 然后由此像线性空间一样, 把有限生成的 Abel 群分解为一系列的循环的 Abel 群直和.

定义 4.1.1 (挠子模 (torsion subgroup)). 对于一个 Abel 群 G, 其挠子模定义如下:

$$tG = \{g \in G : \text{g 是有限阶的}\}$$

若是 G 里的元素全是有限阶的, 即 $tG = G$, 则称 G 是**有挠的 (torsion)**. 若是 G 里的元素是无限阶的, 即 $tG = 0$, 则称 G 是**无挠的 (torsion-free)**.

首先, 一般的 Abel 群 G 未必都是无挠的, 所以通常可以考虑商掉 tG, 从而将有挠的部分和无挠的分开了, 商群 G/tG 是无挠的.

性质 4.1.2. *(1) 商群 G/tG 是无挠的.*

(2) 若 $G \cong H$, 则有 $tG \cong tH, G/tG \cong H/tH$

证明. (1) 设 $x + tG \neq 0$ 有限阶, 则有 $nx + tG = 0$, $nx \in tG$, 于是存在 m, 使得 $mnx = (mn)x = 0$, 其中 $x \in tG$. 这得到 $x + tG = 0$, 矛盾.

(2) 考虑同构映射 $\phi : G \to H$. 对于同构, 限制到 tG 上自然有 $tG \cong \phi(tG)$. 若 $x \in tG$, $\phi(nx) = n\phi(x) = 0$. 于是, $\phi(tG) \subset tH$. 而考虑到同构, 同构会保持元素的阶, 故对任意的 $h \in H$, 对应于相同阶的原像 $g \in tG$, $h = \phi(g) \in \phi(tG)$. 从而, $tH \subset \phi(tG)$, 则有 $tH = \phi(tG)$. 所以, $tG \cong tH$. 而第二个同构只需考虑 $\phi_* : x + tG \mapsto \phi(x) + tH$ 即可.

□

定理 4.1.3 (有限生成 Abel 群关于挠元的直和分解).

(1) 任意的有限生成的无挠的 Abel 群是自由群.

(2) 有限生成的自由 Abel 群 G 的子群 S 是自由的, 且有 $\mathrm{rank}(S) \leq \mathrm{rank}(G)$.

证明. (1) 首先, 要注意的是有限生成的未必是自由的. 就像线性空间一样, 一组向量可以生成一个线性空间. 但这组向量未必就是基. 而存在极大线性无关组保证这组向量中必然有基. 而此处, 有限生成的 Abel 群, 在排除有挠的情况下, 一定会有一组基. 证明使用归纳法. 假设 $G = \langle v_1, v_2, \ldots, v_n \rangle$, 对 n 归纳. 当 $n = 1$, G 为循环群, 而 G 是无挠的, 则 $G \cong \mathbb{Z}$. 从而, G 是自由的. 对于 $G = \langle v_1, \ldots, v_n, v_{n+1} \rangle$, 不妨考虑 $\overline{G} = G/\langle V_{n+1} \rangle$, 通过做商降可以低一个" 维数", 从而实现归纳. 考虑 $\overline{G}$ 的挠子群 $\overline{U}$, 它对应于 G 中的一个子群:

$$U = \{x \in G \mid \text{存在} m \neq 0, mx \in \langle x_{n+1} \rangle\}$$

同样, 根据对应定理, 我们有 $G/U \cong \overline{G}/\overline{U}$. 于是, G/U 与 $\overline{G}/\overline{U}$ 一样是无挠的. 注意到:

$$G/U = \langle v_1 + U, \ldots, v_n + U \rangle$$

由归纳知, G/U 是自由的. 此时意味着直和分解 $G = U \bigoplus G/U$ 成立. 下面, 我们的主要任务是说明 $U \cong \mathbb{Z}^m$. 而事实上, 可以证明这里的 $m = 1$. $x \in U$, 存在 $rx = mv_{n+1}$. 定义同态:

$$\begin{aligned} \phi : U &\to \mathbb{Q} \\ x &\mapsto \phi(x) = m/r \end{aligned}$$

首先, 说明 ϕ 是良定义的. 即如果 $rx = av_{n+1}$, $sx = bv_{n+1}$, 则在 ϕ 的作用下对应于 $a/r, b/s$. 而考虑到 $sav_{n+1} = rbv_{n+1}$ 以及 v_{n+1} 是无限阶的. 所以, 必有 $sa = ra$, $a/r = b/s$. 从而 ϕ 是良定义的. 而 ϕ 是单射, 由此有 $U \cong \mathrm{Im}\,\phi \subset \mathbb{Q}$. 下面, 我们研究 $\mathbb{Q}$ 内任意有限生成的子群的性质. 设

$$D = \langle b_1/c_1, \ldots, b_m/c_m \rangle$$

D 是有限生成的子群, 考虑同态映射:

$$\begin{aligned} f : D &\to \mathbb{Z} \\ d &\mapsto cd \end{aligned}$$

其中, $c = c_1 c_2 \ldots c_m$. 由此 $D \cong \mathrm{Im}\, f \subset \mathbb{Z}$. 事实上, 从 f 的定义可知 $\mathrm{Im}\, f$ 也是 $\mathbb{Z}$ 的子环. 更直接的, 可以把 D 看作 $\mathbb{Z}-$ 模, 以及 f 为 $\mathbb{Z}-$ 同态, 则 $\mathrm{Im}\, f$ 为 $\mathbb{Z}-$ 子模. 即 $\mathrm{Im}\, f$ 是理想, 而 $\mathbb{Z}$ 是主理想整环, 不难看出形如 $m\mathbb{Z}$ 的理想和 $\mathbb{Z}$ 同构. 由此 $\mathrm{Im}\,\phi \cong D \cong \mathrm{Im}\, f \cong \mathbb{Z}$.

(2) 若 R 为主理想整环, 根据定理(2.2.13), R 上的自由模 F, 其任意的子模 H 也是自由的, 且 $\mathrm{rank}(H) \leq \mathrm{rank}(F)$. 此处, Abel 群只是一个特别的 $\mathbb{Z}-$ 模, 所以这是对的. 事实上, 命题中的 "有限生成" 这一条件可以去掉, 结论也成立.

□

推论 4.1.4. *若 Abel 群 G 可由 n 个元素生成, 则其任意子群可以由 n 个或是更少的元素生成.*

证明. 记 $G = \langle g_1, g_2, \ldots, g_n \rangle$, 考虑一个自由 Abel 群 F, 它的基是 $x_1, x_2, \ldots, x_n$, 以及相应的一个满同态 $\phi : F \to G$. 满同态把每个基对应的映过去:$\phi(g_n) = x_n$. 从而, 由对应定理知对于 $S \subset G$, 存在 $\mathrm{Ker}\,\phi \subset F' \subset F$, 使得 $F'/\mathrm{Ker}\,\phi \cong G$. 而 F' 作为自由 Abel 群 F 的子群, 从而其 $\mathrm{rank}(F') \leq n$. 于是, 相应的 G 至多由 n 个元素生成. □

推论 4.1.5. *任意有限生成的 Abel 群 G 可以分解为如下直和:*

$$G = tG \oplus F$$

其中 F 是某个有限生成的自由群.

证明. 当然, 考虑正合列 $0 \to tG \to G \to G/tG \to 0$, 其中由 G/tG 是自由的. 这是因为它是无挠的, 有限生成的, 所以定理(4.1.3)给出. 立即得出上述分解. 其中 $F \cong G/tG$. □

定义 4.1.6 ($p-$ **准素群 (p-primary group)**)**.** 对于群 G 中的任意的一个元素 $a \in G$, a 的阶为 p^k.

定义 4.1.7 (**准素分解 (primary decomposition)**)**.** 设 G, H 为两个挠的 Abel 群 $(tG = G, tH = H)$

(1) G 可以分解成如下直和:

$$G = \bigoplus_p G_p$$

其中, $G_p = x \in G \mid$ 存在$k \in \mathbb{N}, p^k x = 0$.

(2) G, H 同构, 当且仅当对于每个素数 $p, G_p \cong H_p$.

证明. (1) 因为是有挠的, 所以所有的元素都是有限阶的. 对于任意 $g \in G$, 设其阶为 d, 对 d 做因式分解得到 $d = p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m}$. 定义 $r_i = d/p_i^{n_i}$. 由 $p_i^{n_i} r_i x = 0$ 可知 $r_i x \in G_{p_i}$. 易知 $\gcd(r_1, r_2, \ldots, r_m) = 1$, 由此存在一组 s_i, 使得 $\sum_i s_i r_i = 1$. 从而有 $x = \sum_i s_i r_i x \in G_{p_1} + \cdots + G_{p_m}$. 另一方面, 记 $A_i = G_{p_1} + \cdots + \hat{G}_{p_i} + \cdots + G_{p_m}$, 也就

是要说明 $A_i \cap G_{p_i} = 0$. 任取 $x \in A_i \cap G_{p_i}$, 因为 $x \in G_{p_i} \cap A_i$, 所以有 $p^l x = 0, ux = 0$, 其中 $u = \prod_{j \neq i} p_j^{n_j}$. 而由于 p_i^l, u 互素, 于是存在 $s, t \in \mathbb{Z}$, 使得:

$$sp_i^l + tu = 1$$
$$x = (sp_i^l + tu)x = 0$$

(2) 设 $\phi : G \to H$ 是同构, 有 $G_p \cong \phi(G_p)$, 而 $\phi(G_p) \subset H_p$, 但是同构保持阶, 自然这就是 $\phi(G_p) = H_p$. 反过来, 若是给出每个直和分量的同构 $\phi_p : G_p \to H_p$, 可自然诱导出唯一同构:

$$\bigoplus_p G_p \to \bigoplus_p H_p$$
$$\sum_p a_p \mapsto \sum_p \phi_p(a_p)$$

□

定义 4.1.8 (pure subgroup). 设 G 是 $p-$ 准素 Abel 群, 若对任意的 $n \in \mathbb{Z}$, 它的一个子群 S 满足下式:

$$S \cap p^n G = p^n S$$

引理 4.1.9. *若 p 是素数, G 是个有限的 p-准素 Abel 群, 则 G 会有个非零的纯的循环子群, 并且这个子群可以就是由 G 中阶最大的元素生成的.*

证明. 考虑到 G 的有限性, 则 G 中一定会有阶数最大的元素, 不妨设这个元素是 $y \in G$, 设它的阶设 p^l. 下面证明 $S = \langle y \rangle$ 是一个循环纯子群. 取 $s \in S$, 其中 $s = mp^t y$, $\gcd(m, p) = 1$. 假设 $s = p^n a$, $a \in G$, 现在我们需要寻找 $s' \in S$, 使得 $s = p^n s'$. 事实上, 由上述 s 的等式变形得到:

$$s = mp^t y = mp^{(t-n+n)} y = p^n (mp^{t-n} y)$$

于是, 我们有 $s' = mp^{t-n} y$. 下面我们需要说明 $t - n$ 是正数, 否则上述定义非良定义的. 注意到:

$$p^l a = p^{(l-n)} p^n a = p^{l-n} s = p^{l-n} mp^t y = mp^{l-n+t} y$$

由 y 的阶的极大性得到 $l - n + t \leq l$, 从而有 $t - n \geq 0$. □

定义 4.1.10. 对于一个 Abel 群 G 及素数 p, 商群 G/pG 可构成 $\mathbb{F}_p$ 上的线性空间, 则它的维数记为 $\delta(G)$, 即 $\delta(G) = \dim_{\mathbb{F}_p}(G/pG)$. 容易知道, δ 满足以下两个等式:

$$\delta(G \oplus H) = \delta(G) + \delta(H) \tag{4.1}$$

$$(G \oplus H)/p(G \oplus H) = (G \oplus H)/pG \oplus pH \tag{4.2}$$
$$= (G/pG) \oplus (H/pH) \tag{4.3}$$

引理 4.1.11. *若 G 是个有限的 p-准素 Abel 群, 则 $\delta(G)=1$, 当且仅当 G 为非零的循环群.*

证明. 首先, 对于 p-准素 Abel 群而言, 若是 $G=pG$, 则要么 $G=0$ 或者 G 有限. 考虑同态映射 $p: g\mapsto pg$, 若是 $G=pG$, 则 p 是同构, 但是 G 是 p-准素的, 从而 $p^l g=0$. 所以 $\ker p\neq 0$, 矛盾. 于是, 要么 G 形如 $\mathbb{Z}$ 是无限群, 要么是 0. 用商群来看, 就是对于非零有限 p-准素 Abel 群, $G/pG\neq 0$. 那么, 如果 $\delta(G)=1$, 则 G 是循环的. 从而其商群也是循环的, 即同构于 $\mathbb{Z}_p$. 反过来, 如果 $\delta(G)=1$, 显然是同构 $\mathbb{Z}_p$ 的. 由此 G/pG 是循环的, $G/pG=\langle z+pG\rangle$. 考虑到 $\mathbb{Z}_p$ 是单群, 从而 pG 是极大子群. 事实上, pG 是唯一的一个极大子群. 这是因为如果有另一个极大子群 $L\in G$, 考虑商群有 $G/L\cong\mathbb{Z}_p$, 则 $p(g+L)=0$, 于是 $pg\in L$, 即 $pG\subseteq L$. 由 pG 的极大性质可知 $pG=L$. 此时, 任意 G 的一个真子群都将落在 pG 中, 故 $\langle z\rangle\subseteq pG$. 而这导致 G/pG 的生成元为零, 从而矛盾. 而 $\langle z\rangle$ 不是真子群, 且它又非零, 所有 $G=\langle z\rangle$. □

引理 4.1.12. *设 S 是有限 p-准素 Abel 群 G 的子群:*

(1) 若 $S\subset G$, 则 $\delta(G/S)\leq\delta(G)$.

(2) 若 S 是 G 的一个纯子群, 则 $\delta(G)=\delta(S)+\delta(G/S)$.

证明. (1) 首先注意到 $p(G/S)=(pG+S)/S$, 根据对应定理(1.3.16):

$$\frac{G/S}{p(G/S)}\cong\frac{G/S}{(pG+S)/S}\cong\frac{G}{pG+S}$$

最后一个同构是由第三同构定理(1.3.17). 根据 $pG\subset pG+S$, 从而一个满同态的存在:

$$G/pG\to G/(pG+S)$$
$$g+pG\mapsto g+(pG+S)$$

直观上, 商去一个小的群, 当然要比商去一个大的群要" 大". 以用映射的语言是满射. 最后得到:

$$\delta(G)=\dim(G/pG)\geq\dim(G/(pG+S))=\delta(G/S)$$

(2) 考虑上述同态映射的核 $\ker\phi=(pG+S)/pG$. 特别注意, 核 $\ker p$ 也是作为向量空间 G/pG 的子空间. 根据第二同构定理(1.3.15):

$$(pG+S)/pG\cong S/S\cap pG\cong S/pS$$

最后一个同构是用了 S 作为纯子群的性质 $(S\cap pG=pS)$. 由此,

$$\dim((pG+S)/pG)=\delta(S)$$

考虑到 $(pG+S)/pG$ 作为 G/pG 的子空间, 那么做商空间是合法的:

$$\frac{G/pG}{(pG+S)/pG} \cong \frac{G}{pG+S} \cong \frac{G/S}{p(G/S)}$$

由此, 根据向量空间有关商空间的直和的性质, 不难得出:

$$\delta(G) = \delta(G/S) + \delta(S)$$

□

定理 4.1.13 (有限 Abel 群的结构定理). *任意有限 Abel 群可分解为一系列 p-准素循环群的直和.*

证明. 因为是有限的, 所以必然是有挠的, 从而存在准素分解. 设 Abel 群可直和分解为: $G = \bigoplus_p G_p$. 下面, 我们的思路是对 $\delta(G)$ 做归纳: 当 $\delta(G) = 1$ 时, 已证 G 是循环的. 下面进行归纳步骤, 假设 Abel 群最大阶的元素生成的循环群是纯子群, 则有:

$$\delta(G/S) = \delta(G) - \delta(S), S = \langle y \rangle$$

其中 $y \in G$ 为最大阶元. 由此, 根据归纳假设知 $\delta(G/S)$ 是一系列循环群的直和:

$$G/S = \bigoplus_i \langle \overline{x_i} \rangle$$

其中 $\overline{x_i} = x_i + S$. 令 $\overline{g} = g + S \in G/S$, 设其阶为 p^l. 断言, 存在有" 提升"$z \in G$, 其中" 提升" 是指 $z + S = \overline{g} = g + S$ 满足 z 的阶等于 $\overline{g}$ 的阶. 这是因为, 若 g 有阶 p^n, $n \geq l$. 而 $p^l(g+S) = 0, p^l g = s \in S$, 由于 S 的纯性, 从而存在 $s' \in S$, 使得 $p^l g = p^l s'$. 即 $p^l(g - s') = 0$. 令 $z = g - s'$, 我们有 $p^l z = 0, z + S = g + S = \overline{g}$. 对于 $G/S = \bigoplus_i \langle \overline{x_i} \rangle$ 中的每一个 x_i 都考虑其" 提升", 然后由它们去生成群:

$$T = \langle z_1, z_2, \ldots, z_q \rangle$$

现在 $S+T = G$. 注意到, $g = \sum_i x_i + S = \sum_i z_i + S$, 所以 $S+T = G$. 而对于 $y \in S \cap T$, 我们有 $y = \sum_i m_i z_i \in T$, 且

$$\overline{y} = \sum_i m_i \overline{z_i} = \sum_i m_i \overline{x_i} = 0 \in G/S$$

由此得出 $m_i \overline{x_i} = 0$, 而 $z_i, \overline{(x_i)}$ 的阶相同. 由此可得出 $m_i z_i = 0$, $y = 0, S \cap T = 0$, 进而 $G = S \oplus T$. □

定理 4.1.14 (基定理 (Basis Throem)). *任何有限生成的 Abel 群 G 可以分解成一系列的无限循环群与准素循环群的直和.*

证明. 首先, 由于 G 是有限生成 Abel 群. 我们先对 G 做挠元分解 $G = tG \oplus F$, 其中 F 作为自由群, 它可以分解为一系列的无限循环群的直和. 而 tG 作为有挠的群可以进一步进行准素分解 $tG = \bigoplus_p G_p$. 而 G 的有限生成, 则 G_p 自然是有限的, 于是可以由定理(4.1.14)分解成一系列的有限的 p-准素循环群. □

注 49. 事实上, 上述分解 (同构下) 是唯一的. 从而, 我们说一个分解 (无限循环群, $p-$准素循环群) 确定一个有限生成 Abel 群; 一个有限生成 Abel 群确定一个分解. 由此, 我们找到了有限生成 Abel 的一组完全不变量, 从而实现了对 Abel 群的分类.

4.2 有限生成 Abel 群上的基本定理

基定理对有限生成的 Abel 群的结构进行了探索, 而自然的问题是, 基定理给出的有限生成 Abel 群的直和分解是否唯一? 为此, 我们引入了初等因子和不变因子的概念, 并证明了基定理的直和分解唯一性—基本定理.

基定理可以把有限生成的 Abel 群分解一系列的循环群的直和, 其中无限循环群的直和部分同构于 G/tG, 在已知 G 下, 可以唯一确定的; 剩下的要考察的是有限分解的 $p-$ 准素部分. 对于有限部分的 Abel 群, 可以进一步分解有限的各种准素的 Abel 群, 一个很自然的会猜想: 当两个有限 Abel 群同构时, 每种类型的循环直和项的个数应该是相等的. 然而, 这并不成立, 比如有反例:

$$I_{mn} \cong I_m \oplus I_n.$$

既然可以分解, 我们希望可以找出它的特征, 便于对群的结构进一步的探究.

回顾之前的内容, 我们知道 G/pG 是 $\mathbb{F}_p$ 上的线性空间, 且有函数:

$$\delta(G) := \dim_{\mathbb{F}_p}(G/pG).$$

一般的, 有:

$$\delta(p^n G) = \dim(p^n G/p^{n+1}G),$$

记 p^n 阶循环群为 $C(p^n)$.

引理 4.2.1. *设 G 为有限 p-准素 Abel 群, 令 $G = \oplus_j C_j$, 其中每个 C_j 是循环群, 在这些有限循环群中设阶最大的为 p^t. 设 $b_n \geq 0$ 是 $\{C_j\}$ 中 p^n 阶群的个数, 则存在 $t \geq 1$ 使得:*

$$\delta(p^n G) = b_{n+1} + b_{n+2} + \cdots + b_t$$

证明. 设 B_n 是阶为 p^n 的一切 C_j 的直和. 因 G 的阶有限, 故存在某个 t 使得:

$$G = B_1 \oplus \cdots \oplus B_t$$

因 $j \leq n$ 时, $p^n B_j = 0$, 所以 $p^n G = p^{n+1}B_{n+2} \oplus \cdots \oplus p^{n+1}B_t$. 所以存在如下同构:

$$(p^n G)/(p^{n+1}G) \cong (p^n B_{n+1}/p^{n+1}B_{n+1}) \oplus \cdots \oplus (p^n B_t/p^{n+1}B_t)$$

而当 $n < m$ 时, $\delta(p^n B_m/p^{n+1}B_m) = \delta(p^n B_m) = b_m$, 且 δ 对直和保持, 即:

$$\delta(p^n G) = b_{n+1} + \cdots + b_t$$

□

定义 4.2.2. G 是有限 p-准素 Abel 群, p 是素数, 定义:

$$U(n, G) = \delta(p^n G) - \delta(p^{n+1}G)$$

引理(4.2.1)表明,

$$\delta(p^n G) = b_{n+1} + \cdots + b_t$$
$$\delta(p^{n+1}G) = b_{n+2} + \cdots + b_t$$

所以 $U_p(n, G) = \delta(p^n G) - \delta(p^{n+1}G) = b_{n+1}$.

定理 4.2.3 (不同 p-准素分解中同一类型直和因子个数相同). *p 是素数, 则任意两种有限 p-准素有限 Abel 群的循环群直和分解的同一个类型的直和因子有相同的个数. 特别的, 阶为 p^{n+1} 的直和项个数为 $U(n, G) = b_{n+1}$.*

证明. 由基定理(4.1.14), 存在循环子群 C_j, 使

$$G = \oplus C_j.$$

根据引理(4.2.1), 阶为 p^{n+1} 的 C_j 的个数为 $U(n, G)$, 而 $U(n, G)$ 的定义与分解无关. □

推论 4.2.4. *如果 G, H 是有限 p-准素 Abel 群, 则 $G \cong H$ 当且仅当对任意的 $n \geq 0$ 有 $U(n, G) = U(n, H)$.*

证明. 如果 $\varphi : G \to H$ 是同构, 则对任意的 $n \geq 0$, 我们有 $\varphi(p^n G) = p^n H$. 对任意的 $n \geq 0$, φ 导出了 F_p- 向量空间的同构:

$$(p^n G)/(p^{n+1}G) \to (p^n H/p^{n+1}H)$$
$$p^n g + p^{n+1}G \mapsto p^n \varphi(g) + p^{n+1}H$$

由上述同构态射, 知道其维数 δ 相等, 故:

$$\begin{aligned} U(n, G) &= \dim((p^n G)/(p^{n+1}G)) - \dim((p^{n+1}G)/(p^{n+2}G)) \\ &= \dim((p^n H)/(p^{n+1}H)) - \dim((p^{n+1}H)/(p^{n+2}H)) \\ &= U(n, H). \end{aligned}$$

反之, 假定对任意的 $n \geq 0$, 成立 $U(n,G) = U(n,H)$. 设 $G = \oplus C_i$, $H = \oplus C'_j$. 其中, C_i, C'_j 是循环群. 由引理(4.2.1), 每种循环群在直和项中数目相同, 故可依次构造一个 $G \to H$ 的同构. □

定义 4.2.5. 如果 G 是个 $p-$ 准素 Abel 群, 则它的**初等因子 (elementary factors)** 指的是下列序列中的数:

$$U(0,G), U(1,G), \ldots, U(t-1,G)$$

其中, p^t 为 G 的直和项中最高的循环群的阶数.

如果一个有限 $p-$ 准素 Abel 群的初等因子为 $U(0,G), \ldots, U(t-1,G)$, 则 G 就是 $U(0,G)$ 个 $C(p), \ldots, U(t-1,G)$ 个 $C(p^t)$ 的直和. 比如,

$$G = C(p) \oplus C(p) \oplus C(p) \oplus C(p^2) \oplus C(p^4) \oplus C(p^4)$$

G 是一个 p 群, 其 $U(0,G) = 3, U(1,G) = 1, U(2,G) = 0, U(3,G) = 2$. 这时初等因子也可以记成 (p, p, p^2, p^4, p^4), 其中所有数的乘积为 $|\, G \,|$. 下面推广初等因子的定义, 使其对非准素群也有意义.

定义 4.2.6. 如果 G 是一个有限 Abel 群, 则它的**初等因子**为其 p-准素分量 G_p 的初等因子 $U_p(n,G)$.

如果 G 是一个有限 Abel 群, 其阶为 $|\, G \,| = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$, 则 $U_{p_i}(n,G)$ 是同构于 $C(p_i^{n+1})$ 直和因子的个数. 例如,

$$G = C(2) \oplus C(2) \oplus C(4) \oplus C(9) \oplus C(27) \oplus C(27) \oplus C(81)$$

其初等因子为:

$$U_2(0,G) = 2, U_2(1,G) = 1, U_3(0,G) = 0, U_3(1,G) = 1, U_3(2,G) = 2, U_3(3,G) = 1$$

同样的, 可以将 G 记作 $(2, 2, 2^2; 3^2, 3^3, 3^3, 3^4)$, 不同的系数幂用分号隔开.

现在, 我们可以得到了有限 Abel 群结构的一组完全不变量了:

定理 4.2.7 (基定理的直和分解是唯一的). *两个有限 Abel 群 G,H 同构, 当且仅当对每个素数 p, 他们有相同的初等因子. 即在 G, H 的任意两种准素分解循环群中, 每一阶的直和项的个数相同.*

证明. 由准素分解, $G \cong H$ 当且仅当, 对每个素数 p, $G_p \cong H_p$. 由定理(4.2.3)即得到结果. □

进一步, 有如下结论:

定理 4.2.8 (有限生成 Abel 群的基本定理 I). *两个有限生成的 Abel 群 G, H 同构, 当且仅当他们有相同数量的有限循环直和项, 且他们的挠子群有相同的初等因子. 即 G, H 的任何分解为准素核有限循环群的分解中, 每个阶的直和项的个数相同.*

例 4.2.9. 72 阶的 Abel 群有多少? 对 72 进行素数分解有 $72 = 2^3 3^2$; 用初等因子描述分解的可能的组合有:

(1) 3 种可能的 8 阶群: $(2,2,2), (2,4), (8)$.

(2) 2 种可能的 9 阶群: $(3,3), (9)$.

故同构意义下, 有 $3 \times 2 = 6$ 种可能的 72 阶 Abel 群.

下面我们来介绍有限 Abel 群的第二种循环直和分解, 其不涉及准素群:

性质 4.2.10. *每个有限 (可以非准素)Abel 群 G 可分解为如下有限循环群的直和:*

$$G = C(d_1) \oplus C(d_2) \oplus \cdots \oplus C(d_r).$$

其中 $r \geq 1, C(d_j)$ 为 d_j 阶循环群, 且 $d_1 \mid d_2 \mid \cdots \mid d_r$.

证明. 对于 G 的不同准素部分, 其初等因子串可能长度不同, 我们从其中插入一些 $p_i^0 = 1$, 可让他们有相同的长度 r, 因此可作矩阵:

$$Elem(G) = \begin{bmatrix} p_1^{e(11)} & \cdots & p_1^{e(1r)} \\ p_2^{e(21)} & \cdots & p_2^{e(2r)} \\ \cdots & \cdots & \cdots \\ p_m^{e(m1)} & \cdots & p_m^{e(mr)} \end{bmatrix}$$

其中第 i 行是 G_{p_i} 的不同的初等因子, 以 $0 \leq e(i1) \leq e(i2) \leq \cdots \leq e(ir)$ 来排列. 定义:

$$d_j = p_1^{e(1j)} p_2^{e(2j)} \cdots p_m^{e(mj)},$$

则 $e(ij) \leq e(ij+1)$, 于是:

$$d_j = (p_1^{e(1j)} \cdots p_m^{e(mj)}) | (p_1^{1j+1}) \cdots p_m^{e(mj+1)}) = d_{j+1}.$$

最后, 令 $C(d_j) = C(p_1^{e(1j)}) \oplus \cdots \oplus C(p_m^{e(mj)})$, 其为 d_j 阶循环群. □

推论 4.2.11. *每个非循环有限 Abel 群有一个子群, 同构于某个 $C(k) \oplus C(k)$, $k \geq 1$.*

证明. 由性质(4.2.10), $G \cong C(d_1) \oplus C(d_2) \oplus \cdots \oplus C(d_r), r \geq 2$. 因 G 非循环, $d_1 | d_2$, 则 $C(d_2)$ 为一个同构于 $C(d_1)$ 的子群, 故 G 有一个子群同构于 $C(d_1) \oplus C(d_1)$. □

例 4.2.12. 对于前面 $(2,2,2),(3,3)$ 的结构, 其有矩阵:

$$\begin{bmatrix} 2 & 2 & 2 \\ 1 & 3 & 3 \end{bmatrix}$$

不变因子为 $2 \mid 6 \mid 6$.

对于 $(2,4),(3,3)$ 结构的有:

$$\begin{bmatrix} 2 & 4 \\ 3 & 3 \end{bmatrix}$$

其不变因子为 $6 \mid 12$.

对于 $(2,2,2),(9)$ 结构的有:

$$\begin{bmatrix} 2 & 2 & 2 \\ 1 & 1 & 9 \end{bmatrix}$$

其不变因子为 $2 \mid 2 \mid 18$.

定义 4.2.13. 如果 G 是个有限 Abel 群, 且 $G = C(d_1) \oplus C(d_2) \oplus \cdots \oplus C(d_r)$, 其中 $C(d_j)$ 为 d_j 阶循环群, $d_j > 1$, 且 $d_1 \mid d_2 \mid \cdots \mid d_r$, 则 $d_1, \ldots, d_r$ 为 G 的**不变因子 (invariant factors)**. 且 $|G| = d_1 \ldots d_r$.

定义 4.2.14. 如果 G 是有限 Abel 群, e 是使 $eG = \{0\}$ 的最小的正整数, 称 e 为群 G 的**指数 (exponential)**.

推论 4.2.15. *如果 $G = C(d_1) \oplus C(d_2) \oplus \cdots \oplus C(d_r)$ 是一个有限 Abel 群, 其中 $C(d_j)$ 是 d_j 阶循环群, 且 $d_1 \mid \cdots \mid d_r$, 则 d_r 是 G 的指数.*

证明. 因 $d_j | d_r$, 故对任意的 j, 成立 $d_r.C(d_j) = 0$. 所以 $d_r.G = 0$. 对任意的 $1 \le e \le d_r$, $e.C(d_r) \neq 0$, 从而 d_r 是满足条件的最小正整数, 即 G 的指数. □

定理 4.2.16 (有限 Abel 群的基本定理 II). *两个有限 Abel 群同构, 当且仅当他们有相同的不变因子.*

证明. 设 $|G| = p_1^{g_1} \cdots p_m^{g_m}$. 现构造不变因子 $d_j = p_1^{e(1j)} \cdots p_m^{e(mj)}$, 只要用 d_j 构造初等因子, 由基本定理(4.2.8)立即得证. 对任意的 $1 \le j < r$, 注意到:

$$\begin{aligned} d_{j+1}/d_j &= (p_1^{e(1j+1)} \cdots p_m^{e(mj+1)})/(p_1^{e(1j)} \cdots p_m^{e(mj)}) \\ &= p_1^{e(1j+1)-e(1j)} \cdots p_m^{e(mj+1)-e(mj)}. \end{aligned}$$

由算术基本定理, 可以将所有的 p_i 指数算出:

$$e(ir) - e(ir-1), \cdots, e(i2) - e(i1),$$

相加后我们得到 $e(ij)-e(i1)$. 因 Elem(G) 矩阵中, 每一行元素和为 $\mid G_{p_i} \mid = p_i^{g_i}$, 所有元素和为 $\mid G \mid$. 故:

$$\mid G \mid = d_1 \cdots d_r = p_1^{g_1} \cdots p_m^{g_m},$$

$$\mid G \mid / d_1 = (p_1^{g_1} \cdots p_m^{g_m})/(p_1^{e(11)} \cdots p_m^{e(m1)}),$$

从而, 我们可以计算出 $g_i - e(i1)$, 进而 $e(i1)$ 可被表示, 于是 $e(ij)$ 也就得出了. □

定理 4.2.17 (有限生成 Abel 群的基本定理 II). *两个有限生成的 Abel 群 G, H 同构, 当且仅当它们有相同数量的有限循环直和项, 且他们的挠子群有相同的不变因子.*

例 4.2.18. 考虑群 G, 其不变因子是 $2 \mid 6 \mid 6$, 则有

$$\mid G \mid = 72 = 2 \times 6 \times 6 = 2^3 3^2,$$

$$\mathrm{Elem}(G) = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 1 & 9 \end{bmatrix}$$

注 50. 基定理对非有限生成的群不一定成立, 比如 $\mathbb{Q}$.

4.3 PID 上有限生成模的基定理与基本定理

在有限生成 Abel 群的基定理与基本定理基础之上, 我们将有限 Abel 群的结构定理推广到 PID 上的模. 我们将看到这不仅推广了定理, 也推广了定理的证明. 本节将群的语言翻译成模的语言, 并详细证明模版本的准素分解.

定义 4.3.1. 设 M 是 R-模. 如果 $m \in M$, 则它的**阶理想 (order ideal)**(或**零化子 (annihilator)**) 是指:

$$\mathrm{ann}(m) = \{r \in R : rm = 0\}.$$

我们说 m 有**有挠的 (torsion)**, 如果 $\mathrm{ann}(m) \neq \{0\}$; 否则 m 有**无挠的 (torsion—free)**.

当一个交换环 R 看作是它自身上的模时, 它的幺元 1 有无限阶, 这是因为 $\mathrm{ann}(1) = \{0\}$. 阶理想推广了群论中元素的阶的概念.

性质 4.3.2. *若 G 是交换群, 若 $g \in G$ 是有限阶 d, 则 $\mathbb{Z}$ 中的主理想 (d) 同构于 $\mathrm{ann}(g)$, 当 G 被看成 $\mathbb{Z}$-模时.*

证明. 若 $k \in \mathrm{ann}(g)$ 则 $kg = 0$; 因此 $d \mid k$, 则 $k \in (d)$. 另一方面, 若 $n \in (d)$, 则存在 $a \in \mathbb{Z}$, 使得 $n = ad$. 因此 $ng = adg = 0$, $n \in \mathrm{ann}(g)$. □

定义 4.3.3. 若 M 是 R-模, 其中 R 是整环, 则它的**挠子模** tM**(torsion submodule)** 定义为:

$$tM = \{m \in M : ann(m) \neq \{0\}\}$$

性质 4.3.4. 如果 R 是整环和 M 是 R-模, 则 tM 是 M 的子模.

证明. 如果 $m, m' \in tM$, 则存在非零元素 $r, r' \in R$, 使得 $rm = 0$ 和 $r'm' = 0$. 显然, $rr'(m + m') = 0$. 因 R 是整环, $rr' \neq 0$, 从而 $\mathrm{ann}(m + m') \neq \{0\}$; 所以 $m + m' \in tM$. 如果 $s \in R$, 则因 $rsm = 0$, 从而 $r \in \mathrm{ann}(sm)$, 所以 $sm \in tM$. □

注 51. 如果 R 不是整环, 则上述性质不成立.

定义 4.3.5. 设 R 是整环和 M 是 R-模, 则称 M 是**挠**模, 如果 $tM = M$, 而称 M 是**无挠**模, 如果 $tM = \{0\}$.

性质 4.3.6. 设 M 和 M' 都是 R-模, 其中 R 是整环.

(1) M/tM 是无挠的.

(2) 如果 $M \cong M'$, 则 $tM \cong tM'$ 和 $M/tM \cong M'/tM'$.

证明. (1) 若 M/tM 中 $m + tM \neq 0$; 即 m 有无限阶. 如果 $m + tM$ 有有限阶, 则存在某个 $r \in R$ 且 $r \neq 0$ 满足 $0 = r(m + tM) = rm + tM$; 即 $rm \in tM$. 于是存在 $s \in R$ 且 $s \neq 0$ 使得 $0 = s(rm) = (sr)m$. 但因 R 是整环, 所以 $sr \neq 0$, 从而 $\mathrm{ann}(m) \neq \{0\}$, 矛盾.

(2) 如果 $\varphi : M \to M^{'}$ 是同构, 则因对 $rm = 0$ 且 $r \neq 0$ 有 $r\varphi(m) = \varphi(rm) = 0$, 所以 $\varphi(tM) \subseteq tM^{'}$; 因此 $\varphi|tM : tM \to tM^{'}$ 是同构. 易知如下映射为同构:

$$\phi : M/tM \to M^{'}/tM^{'}$$
$$\phi : m + tM \mapsto \varphi(m) + tM^{'}$$

□

性质 4.3.7. 一个 *Abel* 群是有限的, 当且仅当它是有限生成挠 $\mathbb{Z}$-模.

证明. 如果 G 是有限的, 显然是有限生成的, 根据 Lagrange 定理, G 是挠的. 反之, 设 $G = \langle x_1, \ldots, x_n \rangle$, 并存在非零整数 d_i 使得对一切 i, $d_i x_i = 0$. 因此, 每个 $g \in G$ 可以写成:

$$g = m_1 x_1 + \cdots + m_n x_n,$$

其中, 对一切 i, $0 \leq m_i < d_i$. 所以,$| G | \leq \prod_i d_i$, 因此 G 是有限的. □

定义 4.3.8. 如果 M 是 R-模, 则它的**指数 (exponetial)**(或**零化子**) 是指理想:

$$\mathrm{ann}(M) = \{r \in R : rM = \{0\}\}.$$

定理 4.3.9 (PID 上有限生成无挠模是自由的). *如果 R 是 PID, 则每个有限生成无挠 R-模 M 是自由模.*

证明. 参考前文证明 □

定义 4.3.10. 设 R 是 PID 和 M 是 R-模, 如果 $P=(p)$ 是 R 中的非零素理想,. 称 M 为 (p)-**准素 (primary)** 的, 如果对每个 $m\in M$ 存在 $n\geq 1$ 使得 $p^n m=0$. 如果 M 是任意 R-模, 则它的 (p)-**准素分量 (primary components)** 是指:

$$M_p=\{m\in M:\exists n\geq 1, p^n m=0\}.$$

性质 4.3.11. *PID 上的两个挠模 M 和 M' 同构, 当且仅当对每个非零素理想 P, $M_P\cong M'_P$.*

证明. 参考前文证明 □

定理 4.3.12 (准素分解). *每个挠 R-模 M(其中 R 是 PID) 是它的 P-准素分量的直和:*

$$M=\sum_P M_P.$$

证明. 将群版本的证明翻译为模的语言. 如果 $m\in M$ 是非零的, 它的阶理想 $\mathrm{ann}(m)=(d)$, 其中 $d\in R$. 根据唯一因子分解, 存在不可约元素 $p_1,\ldots,p_n$(它们中任两个都不是相伴的) 和正指数 $e_1,\ldots,e_n$ 使得:

$$d=p_1^{e_1}\ldots p_n^{e_n}.$$

于是, 对每个 i,$P_i=(p_i)$ 是素理想, 可定义 $r_i=d/p_i^{e_i}$, 从而 $p_i^{e_i}r_i=d$. 因此, 对每个 i, $r_i m\in M_{P_i}$. 但注意到 $\gcd(r_i,\ldots,r_n)=1$, 从而存在元素 $s_1,\ldots,s_n\in R$, 使得 $1=\sum_i s_i r_i$. 所以,

$$m=\sum_i s_i r_i m\in\left\langle\bigcup_P M_P\right\rangle.$$

对每个素理想 P, 记 $H_P=\langle\bigcup_{Q\neq P} G_Q\rangle$. 只要证明如果 $m\in M_P\cap H_P$, 则 $m=0$. 因 $m\in M_P$, 其中 $P=(p)$, 有某个 $l\leq 0$, 使得 $p^l m=0$. 因 $m\in H_P$, 有 $um=0$, 其中 $u=q_1^{f_1}\ldots q_n^{f_n}$, $Q_i=(q_i)$, $f_i\geq 1$. 但是 p^l 和 u 互素, 因此存在 $s,t\in R$, 使得 $1=sp^l+tu$. 所以:

$$m=(sp^l+tu)m=sp^l m+tum=0.$$

□

我们可以陈述模版本下的基定理和基本定理.

定理 4.3.13 (PID 上有限生成模的基定理). 如果 R 是 *PID*, 则每个有限生成模 M 都是循环模的直和, 其中每个循环项是准素的.

性质 4.3.14. 设 R 是一个 *PID*, 设 M 和 N 是有限生成的挠 R-模. $M \cong N$ 当且仅当它们有相同的初等因子.

定义 4.3.15. M 是有限生成挠 R-模, 其中 R 是 PID. 如果

$$M = R/(c_1) \oplus R/(c_2) \oplus \cdots \oplus R/(c^t),$$

其中 $t \geq 1$ 和 $c_1 \mid c_2 \mid \cdots \mid c_t$, 则 $(c_1), (c_2), \ldots, (c_t)$ 称为 M 的**不变因子 (invariant factors)**.

定理 4.3.16 (PID 上有限生成模的基本定理). 如果 R 是 *PID*, 则两个有限生成 R-模同构, 当且仅当它们的挠子模有相同的不变因子.

4.4 矩阵的特征值与行列式因子

本次讨论班继上次内容, 介绍特征值理论, 我们可以分析, 友阵对应的多项式与特征多项式的关系, 以及特征多项式与不变因子, 初等因子的关系, 进而可以从特征多项式中分解出最小多项式, 再分解出不变因子. 此时, 有理典范型就可以求解, 除此之外, 矩阵的特征多项式与其 Jordan 标准型也有一定关系.

定义 4.4.1. 在 n 维向量空间中可以找到保持任一一维子空间不变, 即存在非零向量 x 对某个标量 α 满足 $Ax = \alpha x$. 此时我们称 α 为 A 的一个**特征值 (eigenvalue)**, 称 x 为 A 的一个**特征向量 (eigenvector)**.

即是说, x 是齐次方程组 $(A - \alpha I)x = 0$ 的非平凡解; 即 $A - \alpha I$ 是非奇异矩阵. 但元素在一个域中的矩阵是非奇异的当且仅当它的行列式为零. 回忆 A 的**特征多项式**是 $\phi_A(x) = \det(xI - A) \in k[x]$, 因此 A 的特征值是 $\phi_A(x)$ 的根. 如果 $\overline{k}$ 是 k 的代数闭包, 则 $\phi_A(x) = \prod_{i=1}^{n}(x - a_i)$, 因此 $\phi_A(x)$ 的常数项为 $(-1)^n \prod_{i=1}^{n} a_i$, $\det(A)$ 是特征值的积.

推论 4.4.2. 设 A 是元素在域 k 中的 n 阶方阵.

(1) A 是奇异的当且仅当 0 是 A 的一个特征值.

(2) 如果 a 是 A 的特征值, 则 α^n 是 A^n 的一个特征值.

(3) 如果 A 是非奇异的且 α 是 A 的一个特征值, 则 $\alpha \neq 0$ 且 α^{-1} 是 A^{-1} 的一个特征值.

证明. (1) 如果 A 是奇异的, 则齐次方程组 $Ax = 0$ 有非平凡解; 即存在非零向量 x 满足 $Ax = 0$. 但这就说明 $Ax = 0x$, 因此 0 是一个特征值.

(2) 如果存在非零向量 v 满足 $Av = \alpha v$. 对 $n \geq 1$ 用归纳法可证明 $A^n v = \alpha^n v$. $A^2\alpha = A\alpha v = \alpha A v = \alpha^2 v$, 则 $A^2 v = \alpha^2 v$, 由此可以类推.

(3) 如果 x 是 A 和 α 的特征向量, 则

$$x = A^{-1}Ax = A^{-1}\alpha x = \alpha A^{-1}x$$

所以, $\alpha \neq 0$ 和 $\alpha^{-1}x = A^{-1}x$.

□

重新回到标准型的理论, 我们有:

定理 4.4.3. *如果 $g(x) \in k[x]$, 则 $\det(xI - C(g)) = g(x)$.*

证明. 如果 $\deg(g) = s \geq 2$, 则有:

$$xI - C(g) = \begin{pmatrix} x & 0 & \cdots & 0 & c_0 \\ -1 & x & \cdots & 0 & c_1 \\ 0 & -1 & \cdots & 0 & c_2 \\ 0 & 0 & -1 & \cdots & c_3 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & \cdots & -1 & x + c_{s-1} \end{pmatrix}$$

对第一行用 Laplace 展开式得

$$\det(xI - C(g)) = x\det(L) + (-1)^{1+s}c_0\det(M)$$

其中 L 是删去第一行和第一列得到的矩阵, M 是第一行和最后一列得到的矩阵. 现在 M 是 $(s-1)\times(s-1)$ 三角矩阵, 对角线上元素是 -1, 而 $L = xI - C((g(x) - c_0)/x)$. 根据归纳假设, $\det(L) = (g(x) - c_0)/x$, 而 $\det(M) = (-1)^{s-1}$. 所以,

$$\det(xI - C(g)) = x[(g(x) - c_0)/x] + (-1)^{(1+s)+(s-1)c_0} = g(x)$$

如果 $R = C(g_1) \oplus C(g_2) \oplus \cdots \oplus C(g_t)$ 是有理标准性, 则

$$xI - R = [xI - C(g_1)] \oplus \cdots \oplus [x - C(g_t)]$$

由引理(4.6.5)有 $\det(B_1 \oplus \cdots \oplus B_t)$, 因此有:

$$\phi_C(x) = \prod_{i=1}^{t} \phi_C(g_i)(x) = \prod_{i=1}^{t} g_i(x)$$

于是, 特征多项式是不变因子的乘积; 域 k 上的 $n \times n$ 矩阵 A 的特征多项式是 $(k^n)^A$ 的类似于有限 Abel 群的阶. □

例 4.4.4. 我们现在证明相似矩阵有相同的特征多项式. 如果 $B = PAP^{-1}$, 则因 xI 和每个矩阵都可交换, 所以有 $P(xI) = (xI)P$, 因此, $P(xI)P^{-1} = xI\ PP^{-1} = xI$. 所以,

$$\begin{aligned}\phi_B(x) &= \det(xI - B) \\ &= \det(PxIP^{-1} - PAP^{-1}) = \det(P[xI - A]P^{-1}) \\ &= \det(P)\det(xI - A)\det(P^{-1}) = \det(xI - A) \\ &= \phi_A(x)\end{aligned} \tag{4.4}$$

由此, 如果 A 相似于

$$C(g_1) \oplus \cdots \oplus C(g_t),\ \phi_A(x) = \prod_{i=1}^{t} g_i(x)$$

所以, 相似矩阵相同的特征值相同重数.

定理 4.4.5 (Hamilton—Caley). *如果 A 是由有特征多项式 $\phi_A = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ 的 $n \times n$ 矩阵, 则 $\phi_A = 0$. 于是:*

$$A^n + b_{n-1}A^{n-1} + b_{n-2}A_{n-2} + \cdots + b_1A + b_0I = 0$$

证明. 根据上面的例子, 可以假定 $A = C(g_1) \oplus \cdots \oplus C(g_t)$ 是有理标准型 (4.6 节), 其中 $\phi_A(x) = g_1(x) * g_2(x) * \cdots * g_t(x)$. 如果把 k^n 看作 $k[x]$-模 $(k^n)^A$. 则由前面的定理知对于一切的 $y \in k^n, g_t(A)y = 0$. 于是, $g_t(A) = 0$. 然而因 $g_i(x) \mid \phi_A(x)$, 所以有 $\phi_A(A) = 0$. □

性质 4.4.6. *最小多项式 $m_A(x)$ 是特征多项式 $\phi_A(x)$ 的因式, 且 A 的每个特征值都是 $m_A(x) = 0$ 的根.*

证明. Hamilton—Caley 定理的证明中(4.4.5), 证明 $m_A(x) \mid \phi_A(x)$, 又在上述例子中有包含 $c_i(x)$ 是 A 的最小多项式, 其中 $c_i(x)$ 是 A 的次数最高的不变因子. 由此, 从事实

$$\phi_A(x) = c_1(x) * c_2(x) * \cdots * c_t(x)(\text{其中} c_1(x) \mid c_2(x) \mid \cdots \mid c_t(x))$$

所以 $m_A(x) = c_t(x)$ 是最小多项式, 且以 A 的每个特征值为根. (当然, 其根的重数可能小于 $\phi_A(x)$ 根的重数) □

推论 4.4.7. *如果 $n \times n$ 矩阵 A 的一切特征值都不同, 则 $m_A(x) = \phi_A(x)$; 即最小多项式与特征多项式相同.*

证明. 因为 $\phi_A(x)$ 的每个根都是 $m_A(x)$ 的根, 即证. □

推论 4.4.8. *(1) $n \times n$ 矩阵 A 相似于一个友矩阵当且仅当 $m_A(x) = \phi_A(x)$.*

(2) 有限 Abel 群 G 是循环的当且仅当它的指数等于它的阶.

证明. (1) 友矩阵 $C(g)$ 只有一个不变因子, 就是 $g(x)$; 但上面例子中把最小多项式等同于最后一个不变因子. 如果 $m_A(x) = \phi_A(x)$, 则根据推论有 A 只有一个不变因子, 就是 $\phi_A(x)$. 因此, A 和 $C(\phi_A(x))$ 有相同的不变因子, 所以它们相似.

(2) n 阶循环群只有一个不变因子, 就是 n; 但推论把指数等同于最后一个不变因子. 如果 G 的指数等同于它的阶 $|G|$, 则 G 只有一个不变因子, 就是 $|G|$. 因此 G 和 $I_{|G|}$ 有相同的不变因子, 从而它们同构.

□

4.5 Jordan 标准型

定义 4.5.1. 设 $a \in k$, k 是个域, 如下定义 Jordan 块:

$$J(a,s) = \begin{pmatrix} a & 0 & 0 & \cdots & 0 & 0 \\ 1 & a & 0 & \cdots & 0 & 0 \\ 0 & 1 & a & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a & 0 \\ 0 & 0 & 0 & \cdots & 1 & a \end{pmatrix}$$

其中, 当 $s = 1$ 时, 定义 $J(a,1) = [a]$.

对 Jordan 块做形如 $J = aI + L$ 的分解, 其中 I 是单位矩阵, L 是主对角线往下以斜线上是 1, 其余是 0 的矩阵. 注意到 I, L 的交换性和 $L^s = 0$ 后, 利用 Newton 的二项式展开给出:

$$J^m = a^m I + \sum_{i=1}^{s-1} \binom{m}{i} a^{m-i} L^i$$

这就对计算矩阵的幂提供了方便. 而事实上, 矩阵必然相似于一种 Jordan 矩阵, 也就是对角线上是 Jordan 块的矩阵, 如果特征多项式可以在 k 中完全分解的话. 这也是本节的核心.

引理 4.5.2. *设 $g(x) = (x-a)^s$, 其友矩阵 $C(g)$ 相似于一个 Jordan 块 $J(a,s)$*

证明. 首先, 定义线性变换:

$$T : k^s \to k^s$$

其中,

$$z \mapsto C(g)z$$

考虑一组基 $v, Tv, T^2v, \ldots, T^{s-1}v$, 其中 v 可以取最平凡的 $(1, 0, \ldots, 0)$. 在这个基下, T 变换对应的矩阵就是 $C(g)$. 接下来, 若取另一个基 $v, (T-aI)v, \ldots, (T-aI)^{s-1}$, 此时可以证明在这个基下 T 对应的矩阵就是 $J(a, s)$:

$$T(T-aI)^j v = (T-aI)^j Tv \tag{4.5}$$

$$= (T-aI)^j (aI + (T-aI))v \tag{4.6}$$

$$= a(T-aI)^j v + (T-aI)^{j+1} v \tag{4.7}$$

其中对于 $j+1 = s$ 而言, Cayley-Hamilton 定理给出 $(T-aI)^s = 0$, 所以最后一项是

$$T(T-aI)^{s-1} = a(T-aI)^{s-1}$$

则得证. □

定理 4.5.3. *设 A 是 $n \times n$ 的矩阵, 矩阵里的元素落在域 k 中, 如果 k 包含了所有的特征值, 则特征多项式可以分解, A 就相似于一些 Jordan 块矩阵的直和.*

证明. 回忆之前的对模的循环分解以及对线性空间上的变换的处理, 首先把 A 看作 n 维线性空间 V 上的线性变换, 进而诱导出一个 $k[x]$-模 V^A. V^A, V 两者作为集合而言是完全一样的, 只是一个我们看作 k-模. 对于看作 $k[x]$-模而言诱导一系列的循环模分解 $\langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \ldots$, 其中, $\mathrm{ann}(v_1) = (p_1)$, $\mathrm{ann}(v_2) = (p_1^2)$. 形如 (p_1) 的循环模是存在的. 而这些循环模直和可以对应转化成线性子空间的直和, 每个线性空间取 $v_1, Av_1, \cdots$ 为一组基. 这样变换 A 在这组基下的矩阵构成一系列矩阵 $C(p_1) \oplus C(p_1^2 \oplus) \ldots$ 的直和. 而条件中所有特征值落在域中, 则特征多项式可以完全分解为一次因式的乘积, 即这些 p_1, p_2 实际上是形如 $(x-a_1), (x-a_2)$ 的结构. 这是因为 $p_1 p_1^2 \cdots$ 的乘积就是特征多项式. 接下来根据引理(4.5.2), 给出这些 $C(p_i^{n_j})$ 就是 Jordan 块. □

上述的论述表明了, 求解 Jordan 矩阵就等于求这些 $p_i^{n_j}$, 也就是求解这些不变因子. 具体求解的一种方法是 n 阶子式法, 这会在 4.7 节介绍. 而值得注意的是这些 Jordan 块在对角线上是可以交换顺序的, 交换次序就是意味着矩阵相似. Jordan 矩阵在交换顺序后是唯一的, 这点从上述推到中可以知道.

定理 4.5.4. *(1) 若 A, B 是 $n \times n$ 的在域 k 上的矩阵, 且域包含所有特征值, 那么 A, B 相似当且仅当它们有相同的初等因子.*

(2) 若矩阵 A 相似于两个 Jordan 标准型 H, H', 则 H, H' 有相同的 Jordan 块.

证明. (1) 这点是显然的, 回忆证明过程, 相同初等因子决定一系列的循环模直和进而决定一系列子空间直和进而决定一个 Jordan 标准型, 反过来也成立. 而 Jordan 标准型在不考虑 Jordan 块的顺序下是唯一的.

(2) 类似.

□

4.6 有理标准型

根据**基定理** (basis theorem) 和**基本定理** (foundenmtal theorem), 我们对主理想整环上的有限生成模进行了分类: R 是 PID, M 是有限生成的 $R-$ 模, 则 M 可以被一组完全不变量进行分类刻画. 基定理表明: 每个有限生成的 $R-$ 模 M 可以分解成一簇循环 $R-$ 模的直和; 基本定理表示: 每一个有限生成 $R-$ 模的循环直和分解由一组完全不变量唯一确定. 由于模本身是一种抽象的结构, 因此我们可以把 PID 上模的结构定理运用到具体的对象:

(1) $R=\mathbb{Z}$, 我们可以得到有限生成的 Abel 群结构定理.

(2) $R=k[x]$, k 是一个域, 我们可以得到域 k 上 n 阶方阵的结构定理: 利用**不变因子**((invariant factor), 在相似意义下进行分类, 两个 n 阶方阵相似, 当且仅当它们具有相同的有理标准型.

(3) $R=k[x]$, k 是一个域, 我们可以得到域 k 上 n 阶方阵的结构定理: 利用**初等因子** (elementary divisor), 在相似意义下进行分类, 两个 n 阶方阵相似, 当且仅当它们具有相同的 Jordan 标准型.

(4) k 是一个域, R 是一个交换环, 借助生成元和生成关系, 我们引入 $R-$ 等价和 Gaussian 等价, 可以对域 k 上的任意矩阵进行分类, 它们相似于同一个 Smith 标准型; 特别的, 借助 Smith 标准型, 我们可以计算 Jordan 标准型的初等因子和有理标准型的不变因子.

在线性代数中, 我们已经知道: k 是一个域, V/k 是域 k 上的线性空间, $T:V\mapsto V$ 为线性变换, 则取定 V 的一组基 $X=\{v_1,v_2,\cdots,v_n\}$, 则线性变换 T 唯一决定了一个 n 阶方阵 A

$$A=(a_{ij})=_X[T]_X=(T(v_1),T(v_2),\cdots,T(V_n)),\quad T(v_j)=\sum_{i=1}^{n}a_{ij}v_i$$

即,

$$T(v_1,v_2,\cdots,v_n)=(T(v_1),T(v_2),\cdots,T(v_n))\quad=(v_1,v_2,\cdots,v_n)A$$

设 Y 为 V 的另一组基, 则 $B=_Y[T]_Y$ 与 A 相似, 即存在可逆矩阵 $P\in \mathrm{GL}(n,k)$, 使得 $B=PAP^{-1}$. 反过来, 若 $B=_Y[T]_Y$, 其中 $P\in\mathrm{GL}(n,k)$, 则存在唯一的线性变换 $T:k^n\mapsto k^n$, 以及 k^n 不同的两组基 X,Y, 使得 $B=_Y[T]_Y$, $A=_X[T]_X$.

线性变换在不同基下的矩阵是相似的; 相似矩阵对应于同一线性变化在不同基下的矩阵. 自然的问题是: 任给两个矩阵 A,B, A,B 相似的充分必要条件是什么? 换句话说, A,B 本身满足何种关系使得它们相似. 线性空间在取定一组基时, 线性变换和矩阵是一一对应的; 于是, 我们可以从线性变换抽象的角度着手研究矩阵的分类; 同时, 注意到矩

阵 (线性变换) 的运算, 本质上是多项式的运算, 因此我们可以考虑域 k 上的线性空间 V 由线性变化诱导出的 $k[x]-$ **模**的结构.

定义 4.6.1. k 是一个域, V 是域 k 上的线性空间, $T : V \mapsto V$ 是 V 上的线性变换. $(V, +)$ 是一个 Abel 群, 在 V 上定义多项式环 $k[x]$ 的数量乘法:

$$k[x] \times V \mapsto V$$

$$(f(x), v) \mapsto f(x)v := (\sum_{i=0}^{n} c_i x^i)v = (\sum_{i=0}^{n} c_i T^i)v = f(T)v$$

其中 $T^0 = Id_V$, T^i 为 T 的第 i 次复合. 域 k 上的线性空间 V 关于自身的加法与上述的数乘构成一个 $k[x]-$ **模, 记为** V^T.

注 52. 设 V/k 是有限维向量空间, $\dim_k V = n$, 则 $k[x]-$ 模 V^T 是**有限生成 (generated finitely) 的挠模 (torsion)**.

(1) V^T 是**有限生成的**: 设 $X = \{v_1, v_2, \cdots, v_n\}$ 是线性空间 V 的一组基, 则 X 可以生成 $k[x]-$ 模 V^T; 即

$$V^T = \langle v_1, v_2, \cdots, v_n \rangle$$

只需要考虑 V^T 的底空间 (underlying space) 的结构.

(2) V^T 是**挠模**: 任取 $v \in V$, $\dim_k V = n$, 则 $v, T(v), T^2(v), \cdots, T^n(v)$ 是线性相关的; 即存在不全为 0 的 $c_i \in k$, 使得

$$\sum_{i=0}^{n} c_i T^i(v) = 0 = f(x)(v)$$

即 $0 \neq f(x) = \sum_{i=0}^{n} c_i x^i \in \mathrm{ann}(v)$. 任意 $v \in V$, 存在非零多项式 $f(x)$, 使得 $\mathrm{ann}(v) = (f(x))$.

(3) 向量空间 k^n 上, 我们也可以类似定义 $k[x]-$ 模: 考虑线性变换 T,

$$T : k^n \mapsto k^n$$

$$v \mapsto Av$$

可以定义 $k[x]$ 上的数量乘法:

$$k[x] \times V \mapsto V$$

$$(f(x), v) \mapsto f(x)v := (\sum_{i=0}^{n} c_i x^i)v = (\sum_{i=0}^{n} c_i A^i)v = f(A)v$$

(4) V/k 是线性空间, X 是线性空间 V 的一组基, $T : V \mapsto V$ 是线性变换, 矩阵 $A =_X [T]_X$ 是线性变换在基 X 下对应的矩阵, 则 $k[x]-$ 模

$$V^T \cong (k^n)^A$$

记线性变换 T 所诱导 k^n 上的 $k[x]-$ 模为 $(k^n)^T$.

定义 4.6.2. k 为一个域, V/k 是线性空间, W 为 V 的子空间. 称 W 为 V 的**不变子空间** (invariant subspace), 若 $\forall \sigma \in \mathrm{End}_k(V), \quad \sigma \mid_W \in \mathrm{End}_k(W)$. 即 $\forall \alpha \in W, \quad \sigma(\alpha) \in W$.

例 4.6.3. k 是一个域, V/k 是线性空间, T 是 V 的线性变换. $\dim_k V = n$, W 为 V^T 的子模, 则 W 作为底空间为 V^T 的不变子空间. 因为任取 $f(x) \in k[x]$, $f(T)W \subseteq W$; 特别的, $T(W) \subseteq W$.

定义 4.6.4. k 是一个域, $A \in \mathrm{Mat}_r(k)$, $B \in \mathrm{Mat}_s(k)$, 则矩阵 A 与 B 的**直和** (direct sum) 为 $(r+s) \times (r+s)$ 方阵:

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

下面一个定理揭示了矩阵直和分解对应于线性空间 (模) 的直和分解.

引理 4.6.5 (V^T **的直和分解诱导线性变换** T **在直和因子中的 (矩阵) 直和分解**). *k 是一个域, V/k 是线性空间, $T \in \mathrm{End}_k(V)$. 如果 $k[x]-$ 模 V^T 可以分解成两个子模 W, W' 的直和:*

$$V^T = W \oplus W'$$

且 $B = \{w_1, w_2, \cdots w_r\}$ 为子模 W 的基, $B' = \{w_1', w_2', \cdots w_s'\}$ 为子模 W' 的基, 则 $B \bigcup B'$ 是 V 的基, 满足矩阵的直和分解:

$$_{B\cup B'}[T]_{B\cup B'} =_B [T \mid_W]_B \bigoplus {}_{B'}[T \mid_{W'}]_{B'}$$

证明. 设 W, W' 为 V^T 的子模, 从而为 V^T 的不变子空间. 即 $T \mid_W \in \mathrm{End}_k(W), T \mid_{W'}$, 因为 $V = W \oplus W'$, 所以 $B \bigcup B'$ 为 V 的一组基; 注意到 $T(w_i) \in W = \langle w_1, w_2, \cdots w_r \rangle$; $T(W_i) \in W' = \langle w_1', w_2', \cdots w_s' \rangle$ 所以

$$_{B\cup B'}[T]_{B\cup B'} = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} = A \oplus B$$

其中, A, B 分别是线性变换限制在子空间 W, W' 对应基 B, B' 的矩阵. □

下面, 我们先分析域 k 上线性空间 V 关于线性变换 $T \in \mathrm{End}_k(V)$ 构成的 $k[x]-$ 模的**循环模**. 对于 PID 上循环模的研究, 就正如对有限 Abel 群分类定理中的循环群的研究一样, 它们是 PID 上有限生成模的直和因子, 是至关重要的.

引理 4.6.6 ($k[x]-$ **模 V^T 上循环模的等价刻画**). *k 是一个域, V/k 是线性空间, $T: V \mapsto V$ 为线性变换; 设 W 为 V^T 的子模, 则 W 是以 $v \in V$ 为生成元的有限阶循环模 $W = \langle v \rangle$, $\mathrm{ann}(v) \neq (0)$, 当且仅当存在 $s \geq 1$, 使得存在 $0 \neq g(x) \in k[x]$, $\deg(g(x)) = s$, $g(x)(v) = 0$, $W \cong k[x]/(g)$; 此时*

$$v, T(v), T^2(v), \cdots, T^{s-1}(v)$$

为 W 的一组基.

证明. ($\Longrightarrow$:) $W =_{k[x]} \langle v \rangle = \{f(x)(v) \mid f(x) \in k[x]\}$; $\mathrm{ann}(v) \neq (0)$, 从而存在

$$g(x) = x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0 \in k[x]$$

使得

$$g(x)(v) = (T^s + \sum_{i=0}^{s-1} c_i T^i)(v) = 0$$

因为 $\mathbb{N}$ 有下确界, 可以选取 $g(x)$ 为 $\{h \in k[x] \mid gv = 0\}$ 中次数最小的首一多项式. 因为 $k[x]$ 为 PID, 故 $\mathrm{ann}(v) = (g(x))$, 记 $\deg(g) = s$. 循环模同构于正则模关于生成元的阶理想的商模, 于是

$$W = \langle v \rangle = k[x]/\mathrm{ann}(v)$$

断言: $v, T(v), T^2(v), \cdots, T^{s-1}(v)$ 是线性无关的. 否则存在非零多项式 $h(x)$, $\deg(h) = s - 1 < s = \deg(g)$, 使得 $h(x)(v) = 0$. 这与 $g(x)$ 的选取矛盾. 同时 $\forall w \in W = \langle v \rangle$, 存在 $f \in k[x]$, 使得 $w = fv$. 由 $k[x]$ 上的带余除法:

$$f = qg + r; \quad \deg(r) < s \text{或者} \deg(r) = 0$$

$$w = fv = (qg + r)v = qgv + rv = rv \in W$$

若 $w = rv \notin W$, 则 $v, T(v), T^2(v), \cdots, T^{s-1}(v), rv$ 线性无关. 这与 s 矛盾.
($\Longleftarrow$:) 首先, 注意到 ${}_{k[x]}\langle v \rangle \subseteq_{k[x]} W$, 只考虑 W 的线性空间结构即可. 反之, 对于任意的 $w \in W$, 存在 $c_i \in k$, 使得

$$w = \sum_{i=0}^{s-1} c_i T^i v$$

令 $g(x) = \sum_{i=0}^{n} c_i x^i$, 则 $w = g(x)v \in \langle v \rangle$. 所以 $W =_{k[x]} \langle v \rangle$. 同时, $\mathrm{ann}(v) \neq (0)$, 这是因为 $v, T(v), T^2(v), \cdots, T^{s-1}(v), T^s(v)$ 是线性相关的. 从而存在 $f(x) \in k[x]$, $\deg(f) = s$, $f(T)v = 0$, $f(x) \in \mathrm{ann}(v)$. □

定义 4.6.7. 设 $g(x)=x+c_0$, 则称 $\mathrm{C}(g)=\begin{pmatrix}-c_0\end{pmatrix}$ 为多项式 $g(x)$ 的**友矩阵** (companion matrix); 如果 $g(x)=x^s+c_{s-1}x^{s-1}+\cdots+c_1x+c_0$, 则称

$$\mathrm{C}(g)=\begin{pmatrix}0&0&\cdots&0&-c_0\\1&0&\cdots&0&-c_1\\0&1&\cdots&0&-c_2\\0&0&1&\cdots&-c_3\\\vdots&\vdots&&\ddots&\\0&0&\cdots&1&-c_{s-1}\end{pmatrix}$$

为 $g(x)$ 的**友矩阵**.

注 53. 友矩阵与域 k 上的首一多项式一一对应: $f(x)\in k[x]$, $\mathrm{C}(f)$ 的最后一列就是 $f(x)$ 的系数. 友矩阵将域 k 上的首一多项式与矩阵联系对应, 称为域 k 上线性空间 V/k 作为 $k[x]-$ 模联系线性变换对应矩阵的桥梁.

引理 4.6.8 ($k[x]-$ **模** V^T **上循环模的诱导的友矩阵对应线性变换** T)**.** *k 是一个域, V/k 是线性空间, $T\in\mathrm{End}_k(V)$, V^T 是 $k[x]-$ 模的循环模, $V^T=\langle v\rangle$. 如果 $\mathrm{ann}(v)=(g)$, 其中 $g(x)=x^s+c_{s-1}x^{s-1}+\cdots+c_1x+c_0$, 则线性空间 V 有一组基 $B=\{v,T(v),T^2(v),\cdots,T^{s-1}(v)\}$, 且线性变换 T 在基 B 下的矩阵为多项式 $g(x)$ 的友矩阵 ${}_B[T]_B=\mathrm{C}(g)$.*

证明. 根据 $k[x]-$ 循环模的等价刻画, B 是线性空间 V 的一组基. 同时, 注意到

$$T(T^i(v))=T^{i+1}(v);\quad i<s-1$$

$$T(T^{s-1})(v)=T^s(v)=-\sum_{i=0}^{s-1}c_iT^i(v)$$

即

$$T(v,T(v),T^2(v),\cdots,T^{s-1})=(v,T(v),T^2(v),\cdots,T^{s-1})\begin{pmatrix}0&0&\cdots&0&-c_0\\1&0&\cdots&0&-c_1\\0&1&\cdots&0&-c_2\\0&0&1&\cdots&-c_3\\\vdots&\vdots&&\ddots&\\0&0&\cdots&1&-c_{s-1}\end{pmatrix}$$

于是,

$${}_B[T]_B=\mathrm{C}(g)$$

□

下面, 我们对 $k[x]-$ 模 V^T 使用 PID 上有限生成模的结构定理 (Foundenmtal theroem: invariant factors).

定理 4.6.9 (n **阶方阵的结构定理 (不变因子)**).

(1) k *是一个域,* $A \in \mathrm{Mat}_n(k)$ *是域* k *上的* n *阶方阵. 如果*

$$(k^n)^A = W_1 \oplus W_2 \oplus \cdots \oplus W_r$$

W_i *为* $k[x]$ *上的循环模,* $\mathrm{ann}(W_i) = (g_i) = \{g \in k[x] | gW_i = 0\}$*, 则* A *相似于一系列友矩阵的直和:*

$$A \cong C(g_1) \oplus C(g_2) \oplus \cdots \oplus C(g_r)$$

(2) k *是一个域,* $A \in \mathrm{Mat}_n(k)$ *是域* k *上的* n *阶方阵. 存在* $k[x]$ *上的首一多项式* $g_1(x), g_2(x), \cdots, g_r(x)$ *满足*

$$g_1 | g_2 | \cdots | g_r$$

使得矩阵 A *相似于* $C(g_1) \oplus C(g_2) \oplus \cdots \oplus C(g_r)$.

证明. (1) : 考虑向量空间 k^n 上的线性变换 $T : k^n \mapsto k^n$. $T(y) = Ay, \quad y \in k^n$. 作为 $k[x]-$ 模, 根据 PID 上有限生成模的结构定理, $(k^n)^A$ 可以分解成一些循环模的直和:

$$(k^n)^A = W_1 \oplus W_2 \oplus \cdots \oplus W_r$$

对于每一个循环模 W_i, $\mathrm{ann}(W_i) = (g_i) \neq (0)$, 根据 $k[x]-$ 循环模的等价刻画: 存在一簇关于 W_i 作为底空间的基 B_i, 使得 $T|_{W_i}$ 在 B_i 下的矩阵是 $\mathrm{C}(g_i)$. 同时 $B = \bigcup_{i=1}^{r} B_i$ 是 V 的一组基, 根据 $k[x]-$ 模直和分解诱导矩阵分解:

$${}_B[T]_B = \bigoplus_{i=1}^{r} {}_{B_i}[T|_{W_i}]_{B_i}$$

线性变换在不同基下的矩阵相似, 故 A 与系列友矩阵直和相似.
(2) : $k[x]-$ 模 V^T 是有限生成的挠模, 根据 PID 有限生成模的基本定理 (不变因子):

$$(k^n)^A = W_1 \oplus W_2 \oplus \cdots \oplus W_r$$

W_i 为 $k[x]$ 上的循环模, 其中 $\mathrm{ann}(W_i) = (g_i) \neq (0)$, 且有不变因子:

$$g_1 | g_2 | \cdots | g_r$$

□

定义 4.6.10. R 是域 k 上的矩阵, 若存在域 k 上的首一多项式: $g_1(x), g_2(x), \cdots, g_r(x)$ 满足:

$$g_1|g_2|\cdots|g_r$$

使得

$$R = C(g_1) \oplus C(g_2) \oplus \cdots \oplus C(g_r)$$

则称 R 的上述友矩阵直和分解为 R 的**有理标准型** (rational canonical form). 若矩阵 A 相似于矩阵 R, 此时称 $g_1(x), g_2(x), \cdots, g_r(x)$ 为矩阵 A 的**不变因子** (invariant factor).

注 54. 关于有理标准型的定义来源, 可以做以下的阐述

(1) **rational(有理) 一词的来源:** E/k 是域扩张, 对于 $\forall e \in E\backslash k$, 我们称元素 e 是**无理的** (irrational), 我们称基域 k 为**有理域**, 这是代数数论中实数域 $\mathbb{R}$ 里那些不在 $\mathbb{Q}$ 的元素推广. 对于有理标准型, 其所有元素均在 k 中, 而不在 k 的扩域中. 相比而言, 对应 Jordan 标准型, 矩阵的特征值可以不在域 k 中.

(2) **canonical(典范) 一词来源:** canonical 来源于宗教观念, 表示虔诚的祈祷者. 数学中指由一般法则或公式给出的结果.

我们已经证明, 域 k 上的 n 阶方阵相似于一个有理标准型, 具有不变因子. 自然的问题是, 不变因子是否具有唯一性, 换句话说, 不变因子是否为 n 阶方阵的完全不变量. 下面的定理给出肯定的回答.

定理 4.6.11 (有理标准型不变因子的唯一性).
(1) n 阶方阵 A, B 相似, 当且仅当 A, B 具有相同的不变因子.
(2) 任何一个方阵 A 都同构于唯一一个有理标准型.

证明. (1) : A 与 B 相似, 当且仅当 $(k^n)^A \cong (k^n)^B$, 当且仅当 $(k^n)^A$ 与 $(k^n)^B$ 具有相同的不变因子.
(2) : 设 $C(g_1) \oplus C(g_2) \oplus \cdots \oplus C(g_r)$ 和 $C(h_1) \oplus C(h_2) \oplus \cdots \oplus C(h_t)$ 为矩阵 A 的有理标准型, 则根据有理标准型的推导和 $k[x]-$ 循环模的等价刻画有:

$$k[x]/(g_1) \oplus k[x]/(g_2) \oplus \cdots \oplus k[x]/(g_r) \cong (k^n)^A$$

$$[k[x]/(h_1) \oplus k[x]/(h_2) \oplus \cdots \oplus k[x]/(h_t) \cong (k^n)^A$$

所以, $t = h; g_i = h_i$. □

推论 4.6.12. *K/k 是一个域扩张, $A, B \in \mathrm{Mat}_n(k)$ 为 k 上的 n 阶方阵. 如果 A, B 在 K 上相似, 则 A, B 在域 k 上相似. 即如果存在非奇异矩阵 $P \in \mathrm{Mat}_n(K)$, 使得 $B = PAP^{-1}$, 则存在非奇异矩阵 $Q \in \mathrm{Mat}_n(k)$, 使得 $B = QAQ^{-1}$.*

证明. 设 $g_1, g_2, \cdots, g_r$ 为 A 作为域 k 上的不变因子, $G_1, G_2, \cdots, G_r$ 为 A 作为域 K 上的不变因子, 因为 $k \subseteq K$, 根据不变因子的唯一性 $\{g_1, g_2, \cdots, g_r\}$ 与 $\{G_1, G_2, \cdots, G_r\}$ 在 k 上是一致的. A, B 在 K 上相似, 则在 K 上具有相同的不变因子, 而 A, B 的不变因子均在 k 中, 所以 A, B 在 k 上是相似的. □

注 55.

(a) k 为一个域, $\bar{k}$ 是 k 的代数闭包, $A, B \in \mathrm{Mat}_n(k)$, 则 A, B 在域 k 上相似, 当且仅当 $\bar{k}$ 上相似.

(b) $A, B \in \mathrm{Mat}_n(\mathbb{R})$, 存在 $P \in \mathrm{GL}(n, \mathbb{C})$, 使得 $B = PAP^{-1}$, 则存在 $Q \in \mathrm{GL}(n, k)$, 使得 $B = QAQ^{-1}$.

4.7 Smith 正规型

现在面临一个问题: 如何计算一个给定矩阵的不变因子和初等因子? 在这一节我们将给出计算的算法. 特别地, 我们可以计算最小多项式. 我们将从模的角度讨论域 k 上的 n 阶矩阵, 从而开始本节的讨论.

性质 4.7.1. *对于任意的环 R, 每个左 R-模 M 都是一个自由左 R-模的商. 此外, M 是有限生成的当且仅当 F 可被选为有限生成的.*

证明. 设 F 是 $|M|$ 个 R 的复制的直和 (从而 F 是自由左 R-模), 并且设 $\{x_m\}_{m \in M}$ 是 F 的基. 则对于任意的 $m \in M$, 存在一个 R-映射:

$$g : F \to M$$

$$x_m \mapsto m$$

g 是满射, 故 $F/\ker g \cong M$. 如果 M 是有限生成的, 则 $M = \langle m_1, \cdots, m_n \rangle$. 如果我们选择 F 是有基 $\{x_1, \cdots, x_n\}$ 的自由左 R-模, 则态射 $g : F \to M$ 使得 $g(x_i) = m_i$ 是一个满射, 因

$$\mathrm{Im}\, g = \langle g(x_1), \cdots, g(x_n) \rangle = \langle m_1, \cdots, m_n \rangle = M.$$

逆命题是显然的, 因为任意有限生成模的像是有限生成的. □

推论 4.7.2. *设 R 是一个环. 给定一个左 R-模 M, 则存在正合列:*

$$F' \xrightarrow{h} F \xrightarrow{g} M \longrightarrow 0$$

其中 F 和 F' 是自由左 R-模.

证明. 存在自由左 R-模 F 和满的 R-映射 $g : F \to \ker g$. 因为 $\mathrm{Im}\, h = \ker g$, 我们可以假定存在该正合列. □

定义 4.7.3. 给定一个环 R, 一个左 R-模 M 和一个正合列

$$F' \xrightarrow{h} F \xrightarrow{g} M \longrightarrow 0 \ ,$$

其中 F' 和 F 是自由左 R-模, 则 M 的一个**表现 (presentation)** 是一个有序对

$$(X|Y),$$

其中 X 是 F 的一个基, Y 生成 $\operatorname{Im} h \subseteq F$, 且 $F/\langle Y\rangle \cong M$. 我们称 X 为 M 的**生成元 (generators)**, $\langle Y\rangle$ 为 M 的**关系 (relations)**.

在 PID 中, 情况会更加便于讨论.

推论 4.7.4. *设 R 是一个 PID. 给定一个 R-模 M, 存在一个正合列*

$$0 \longrightarrow F' \xrightarrow{i} F \xrightarrow{g} M \longrightarrow 0,$$

其中 F' 和 F 是自由 R-模.

证明. 因为 R 是一个 PID, 每个自由 R-模的子模都是自由的. □

定义 4.7.5. 设 R 是一个交换环并且设 $\phi : R^t \longrightarrow R^n$ 为一个 R-映射, 其中 R^t 和 R^n 是自由 R-模. 如果 $Y = \{y_1, \cdots, y_t\}$ 是 R^t 的一个基, $Z = \{z_1, \cdots, z_n\}$ 是 R^n 的一个基, 则 ${}_Z[\phi]_Y$ 是一个 R 上的 $n \times t$ 阶矩阵, 其第 i 列为 $\phi(y_i)$ 的坐标,

$$\phi(y_i) = \sum_{j=1}^{n} a_{ji} z_j.$$

矩阵 ${}_Z[\phi]_Y$ 称为 $M \cong \operatorname{Coker}\phi = R^n/\operatorname{Im}\phi$ 的**表示矩阵 (presentationn matrix)**.

下面我们比较不同基下的表现矩阵.

性质 4.7.6. *设 $\phi : R^t \to R^n$ 为自由模之间的 R-映射, 其中 R 为交换环. 选择 R^t 的基 Y 和 Y', R^n 的基 Z 和 Z'. 则存在可逆矩阵 P 和 Q 使得*

$$\Gamma' = Q\Gamma P^{-1},$$

其中 $\Gamma' = {}_{Z'}[\phi]_{Y'}$, $\Gamma = {}_Z[\phi]_Y$ 为对应的表现矩阵. 相反的, 如果 Γ 和 Γ' 为 $n \times t$ 阶矩阵, 且存在某个可逆矩阵 P 和 Q 满足 $\Gamma' = Q\Gamma P^{-1}$, 则存在一个 R-映射 $\phi : R^t \to R^n$, R^t 的基 Y 和 Y', R^n 的基 Z 和 Z', 使得 $\Gamma = {}_Z[\phi]_Y$, $\Gamma' = {}_{Z'}[\phi]_{Y'}$.

证明. 由公式

$$({}_Z[S]_Y)({}_Y[T]_X) = {}_Z[ST]_X,$$

即得, 其中 $T : V \to V'$,$S : V' \to V''$ 且 X, Y, Z 分别为 V, V', V'' 的基. □

定义 4.7.7. 交换环 R 上的两个 $n\times t$ 阶矩阵是 **R-等价 (R-equivalent)** 的, 如果存在 R 上的可逆矩阵使得

$$\Gamma' = Q\Gamma P.$$

显然,R-等价关系是集合上的等价关系.

推论 4.7.8. *设 M, M' 为交换环 R 上的 R-模. 假定存在正合列*

$$R^t \xrightarrow{\lambda} R^n \xrightarrow{\pi} M \longrightarrow 0$$

和

$$R^t \xrightarrow{\lambda'} R^n \xrightarrow{\pi'} M' \longrightarrow 0,$$

并且 Y, Y' 为 R^t 的基, Z, Z' 为 R^n 的基. 如果 $\Gamma =_Z [\lambda]_Y, \Gamma' =_{Z'} [\lambda']_{Y'}$ 为 R-等价的, 则 $M \cong M'$.

证明. 因为 Γ, Γ' 是 R-等价的, 故存在可逆矩阵 P, Q 使得 $\Gamma' = Q\Gamma P - 1$. 现在 Q 定义了一个 R-同构 $\theta : R^n \to R^n$, P 决定了一个 R-同构 $\phi : R^t \to R^t$. 等式 $\Gamma' = Q\Gamma P^{-1}$ 给定了一个交换图

$$\begin{array}{ccccccc} R^t & \xrightarrow{\lambda} & R^n & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \theta} & & \vdots{\scriptstyle v} & & \\ R^t & \xrightarrow{\lambda'} & R^n & \xrightarrow{\pi'} & M' & \longrightarrow & 0. \end{array}$$

定义一个 $R-$ 映射 $v : M \to M'$ 如下. 如果 $m \in M$ 则由 π 是满射给出了一个元素 $u \in R^n$ 满足 $\pi(u) = m$; 令 $v(m) = \pi'\theta(u)$. 则 v 是一个良定义的同构. □

如果 V 是域 k 上的线性空间, 我们可以由线性变换 $T : V \to V$ 构造一个 $k[x]$-模 V^T. 对于每一个 $f(x) = \sum c_i x^i \in k[x]$ 和 $v \in V$, 定义 $fv = \sum_i c_i T^i(v)$. 特别地, 如果 $V = k^n$,A 为 k 上的 n 阶矩阵, 则由 $T(v) = Av$ 定义的 $T : V \to V$ 是线性变换, $k[x]$-模 V^T 记为 V^A. 此时,V^A 中标量乘法由

$$fv = \sum_i c_i A^i v$$

定义, 其中 $f(x) = \sum c_i x^i, v \in V$. 下面我们给出 $k[x]$-模 V^A 的一种更好的表达.

定理 4.7.9 (特征序列 (Characteristic Sequence)). *设 V 是域 k 上的 n 维线性空间, 设 $A = [a_{ij}]$ 为域 k 上的 n 阶矩阵.*
(1) 则存在一个 $k[x]$-模的正合列

$$0 \longrightarrow k[x]^n \xrightarrow{\lambda} k[x]^n \xrightarrow{\pi} V^A \longrightarrow 0.$$

(2) 上述正合列的表示矩阵在 $k[x]^n$ 的标准基下为 $xI - A$.

证明. (1) 设 $Y=\{y_1,\cdots,y_n\}$ 为 V 的一个基, $E=\{e_1,\cdots,e_n\}$ 为标准基. 在直和

$$F=k[x]^n$$

中的每个元素 w 都有唯一的表达式 $w=f_1(x)e_1+\cdots+f_n(x)e_n$, 其中 $f_i(x)=c_{i0}+c_{i1}x+c_{i2}x^2+\cdots\in k[x]$. 代入并合并同类项得:

$$w=u_0+xu_1+x^2u_2+\cdots,$$

其中每个 u_j 为 $e_1,\cdots,e_n$ 的一个 k-线性组合, 即 $u_j\in k^n$. 设 $U\subseteq F$ 为 $e_1,\cdots,e_n$ 的所有 k-线性组合的子集, 因此 F 中的元素 w 可以看作系数在 U 中的多项式.

(a) 定义 $\pi:F\to V^A$ 为

$$\pi(x^ju)=A^jv,$$

其中 $u=c_1e_1+\cdots+c_ne_n\in U$, v 为列向量 $(c_1,\cdots,c_n)^T$.

(b) π 为 $k[x]$-映射:

$$\pi(x(x^ju))=\pi(x^{j+1}u)=A^{j+1}v=xA^jv=x\pi(x^ju).$$

(c) $\pi|U:U\to V$ 为同构:

如果 $u\in U$, 则 $u=c_1e_1+\cdots+c_ne_n,\pi:u\mapsto A^0v=v=c_1y_1+\cdots+c_ny_n$.

(d) π 是满射:

由 (c), 因 V^A 和 V 作为集合是一样的.

(e) 定义 $\lambda:F\to F$ 为

$$\lambda(x^ju)=x^{j+1}u-x^jAu.$$

(f) λ 为 $k[x]$-映射:

$$\begin{aligned}\lambda(x(x^ju))&=\lambda(x^{j+1}u)\\&=x^{j+2}u-x^{j+1}Au\\&=x(x^{j+1}u-x^jAu)\\&=x\lambda(x^ju).\end{aligned}$$

(g) $\operatorname{Im}\lambda\subseteq\ker\pi$:

$$\pi\lambda(x^ju)=\pi(x^{j+1}u-x^jAu)=A^{j+1}v-A^jAv=0.$$

(h) $\ker\pi\subseteq\operatorname{Im}\lambda$:

如果 $w\in\ker\pi$, 则 $w=\sum_{j=0}^m x^ju_j$, 其中 $\sum_{j=0}^m A^jv_j=0$; 由 (c), $\sum_{j=0}^m A^ju_j=0$. 现在

$$w=w-\sum_{j=0}^m A^ju_j=\sum_{j=0}^m(x^ju_j-A^ju_j).$$

因 $x^0u_0 - A^0u_0 = u_0 - u_0 = 0$, 我们可以假设当 $j \geq 1$ 时:

$$w = \sum_{j=1}^{m}(x^j u_j - A^j u_j).$$

但是, 对于每一个 $j \geq 1$:

$$\begin{aligned} x^j u_j - A^j u_j &= \sum_{l=0}^{j-1}(x^{j-l}A^l u_j - x^{j-l-1}A^{l+1}u_j) \\ &= (x^j u_j - x^{j-1}Au_j) + (x^{j-1}Au_j - x^j A^2 u_j) + \cdots . \end{aligned}$$

因为 $x^{j-l}A^l u_j - x^{j-l-1}A^{l+1}u_j$ 显然在 $\operatorname{Im}\lambda$ 中, 故 $w \in \operatorname{Im}\lambda$.

(i) λ 是单射: 假定 $w' = \sum_{i=1}^{m} x^j u_j \in \ker\lambda$, 即 $\lambda(w') = 0$. 可以假定 $x^m u_m \neq 0$, 故 $u_m \in k^n$ 非零. 现在 $k[x]$ 是一个自由 $k-$ 模, 其基为 $\{1, x, x^2, \cdots\}$. $x^{m+1}u_m \neq 0$. 现在

$$0 = \lambda(w') = \sum_{j=0}^{m}(x^{j+1}u_j - x^j Au_j),$$

故

$$x^{m+1}u_m = -x^m Au_m - \sum_{j=0}^{m-1}(x^{j+1}u_j - x^j Au_j).$$

将 $k[x]$ 看作基为 $\{x^i : i \geq 0\}$ 的自由 $k-$ 模, 而

$$0 \neq x^{m+1}u_m \in \langle x^{m+1}\rangle \cap \bigoplus_{j=0}^{m}\langle x^j\rangle = \{0\}.$$

因此 $u_j = 0, w' = 0$, 故 λ 为单射.

(2) 设 ${}_E[\lambda]_E$ 第 i 列元素为 $\lambda(e_i)$, 则:

$$\begin{aligned} \lambda(e_i) &= xe_i - Ae_i \\ &= xe_i - \sum_j a_{ij}e_j \\ &= \sum_j x\delta_{ij}e_j - \sum_j a_{ji}e_j \\ &= \sum_j (x\delta_{ij} - a_{ji})e_j. \end{aligned}$$

因此表示矩阵 ${}_E\lambda_E = xI - A$.

□

推论 4.7.10. *域 k 上的两个 n 阶矩阵相似当且仅当矩阵 $\Gamma = xI - A, \Gamma' = xI - B$ 是 $k[x]$-等价的.*

证明. 如果 A 和 B 相似, 则存在 k 上的非奇异矩阵 P 使得 $B = PAP^{-1}$. 但

$$P(xI - A)P^{-1} = xI - PAP^{-1} = xI - B,$$

故 $xI - A, xI - B$ 是 $k[x]$-等价. 相反地, 假定矩阵 $xI - A, xI - B$ 是 $k[x]$-等价的, 则 $(k[x]^n)^A, (k[x]^n)^B$ 是有限生成的 $k[x]$-模, 表示矩阵分别为 $xI - A, xI - B$. 而 $k[x]$-模 $(k^n)^A \cong (k^n)^B$, 故 A, B 相似. □

在下面的内容中我们将矩阵 A 的第 i 行记为 $\mathrm{ROW}(i)$, 第 j 列记为 $\mathrm{COL}(j)$.

定义 4.7.11. 交换环 R 上的 $n \times t$ 阶矩阵 A 有三种**初等行变换 (elementary row operations)**:

(1) 用 R 中单位乘 $\mathrm{ROW}(j)$.

(2) 用 $\mathrm{ROW}(i) + c\,\mathrm{ROW}(j)$ 代替 $\mathrm{ROW}(i)$, 其中 $j \neq i, c \in R$; 即将 $c\,\mathrm{ROW}(j)$ 加到 $\mathrm{ROW}(i)$ 上.

(3) 交换 $\mathrm{ROW}(i), \mathrm{ROW}(j)$.

类似的也有三种**初等列变换 (elementary column operations)**.

容易验证, 第三类变换可由前两类变换得到.

定义 4.7.12. 初等矩阵 (elementary matrix) 指的是单位矩阵经过有限次初等行变换得到的矩阵.

显然初等矩阵都是可逆的, 其逆矩阵是同类的初等矩阵. 初等矩阵的乘积仍然是初等矩阵.

定义 4.7.13. 设 R 为交换环, 则称两个 $n \times t$ 阶矩阵 Γ, Γ' 是 **Gauss 等价 (Gaussian equivalent)** 的, 如果存在初等行列变换的序列:

$$\Gamma = \Gamma_0 \longrightarrow \Gamma_1 \longrightarrow \cdots \longrightarrow \Gamma_r = \Gamma'.$$

Gauss 等价是一种等价关系. 如果 Γ', Γ 是 Gauss 等价的, 则存在矩阵 Q, P 为初等矩阵的乘积, 使得 $\Gamma' = Q\Gamma P$. 特别地, 两个矩阵 Gauss 等价必然 R-等价. 下面我们将会见到, 当 R 为 Euclid 环时, 逆命题也正确.

定理 4.7.14 (Smith 正规型 (Smith Normal Form)). *Euclid 环 R 上的非零 $n \times t$ 阶矩阵 Γ 的 Gauss 等价于形如下形式的矩阵:*

$$\begin{bmatrix} \sum & 0 \\ 0 & 0 \end{bmatrix}$$

其中 $\sum = \mathrm{diag}(\sigma_1, \cdots, \sigma_q), \sigma_1 | \sigma_2 | \cdots | \sigma_q$ 非零.

证明. 如果 $\sigma \in R$ 非零, 设其在 Euclid 环 R 中的次数为 $\partial(\sigma)$. 在与矩阵 Γ Gauss 等价的所有矩阵的非零元素中, 设 σ_1 有最小的次数, 设 Δ 是与 Γ Gauss 等价并以 σ_1 作为 ij 元的矩阵. 我们证明对于在 Δ 的 ROW(k) 中的所有 $\eta_{kj}, \sigma_1|\eta_{kj}$. 如果不成立, 则存在 $j \neq l, \eta_{kj} = \kappa\sigma_1 + \rho$, 其中 $\partial(\rho) < \partial(\sigma_1)$. 将 COL$(j)$ 加上 $(-\kappa)$ COL(l) 得到矩阵 Δ' 以 ρ 为元素. 而 Δ', Γ Gauss 等价, 其有次数小于 $\partial(\sigma_1)$ 的元素 ρ, 矛盾. 同理 σ_1 整除其所在列的元素. 我们证明 σ_1 整除 Δ 中的每个元素. 设 a 与 σ 不在同一行或列. 我们考虑子矩阵:

$$\begin{bmatrix} a & b \\ c & \sigma_1 \end{bmatrix}$$

其中 $b = u\sigma_1, c = v\sigma_1$. 现在用 ROW$(1)$ + $(1-u)$ ROW$(2) = [a + (1-u)c, \sigma_1]$ 代替 ROW(1). 因为新矩阵与 Δ Gauss 等价, 故 $\sigma_1|(a + (1-u)c)$ 而 $\sigma_1|c$, 故 $\sigma_1|a$. 所以 σ_1 整除 Γ 中所有元素. 下面我们进一步一般化矩阵 Γ. 通过交换, 存在以 σ_1 作为 $1,1$ 元且与 Γ Gauss 等价的矩阵. 如果 η_{1j} 是第一行中另一元素, 则 $\eta_{1j} = \kappa_j\sigma_1$. 将 COL$(j)$ 加上 $(-\kappa_j)$ COL(1) 得到一个新矩阵, 其 $1, j$ 元为 0. 因此我们可以假定 Γ 以 σ_1 为 $1,1$ 元, 且第一行其余元素为 0. 下面我们对行数 $n \geq 1$ 作归纳. 如果 $n = 1$, 我们已经证明 $1 \times t$ 阶矩阵 Gauss 等价于 $[\sigma_1\ 0 \cdots 0]$. 对于归纳步, 我们可以假定 σ_1 为 $1,1$ 元, 第一行其余元素为 0. 因 σ_1 整除第一列的所有元素, Γ Gauss 等价于第一列其余元素也为 0 的矩阵. 因此 Γ Gauss 等价于矩阵形如 $\begin{bmatrix} \sigma_1 & 0 \\ 0 & \Omega \end{bmatrix}$. 由假设, 矩阵 Ω Gauss 等价于矩阵 $\begin{bmatrix} \Sigma' & 0 \\ 0 & 0 \end{bmatrix}$, 其中 $\Sigma' = \mathrm{diag}(\sigma_2, \cdots, \sigma_q), \sigma_2|\sigma_3| \cdots |\sigma_q$. 因此 Γ Gauss 等价于 $\begin{bmatrix} \sigma_1 & 0 & 0 \\ 0 & \Sigma' & 0 \\ 0 & 0 & 0 \end{bmatrix}$, 故 σ_1 整除该矩阵中所有元素. □

定义 4.7.15. 上述定理中的 $n \times t$ 阶矩阵 $\begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix}$ 称为 Γ 的 **Smith 正规型 (Smith normal form)**.

定理 4.7.16. *设 R 是一个 Euclid 环.*

(1) R 上的 n 阶矩阵 Γ 是初等矩阵的乘积.

(2) R 上的两个矩阵 Γ, Γ' 是 R-等价的当且仅当 Gauss 等价.

证明. (1) Γ Gauss 等价于 Smith 正规型 $\begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix}$, 其中 Σ 是对角矩阵. 因为 Γ 是可逆矩阵, 其中没有零矩阵, 故 Γ Gauss 等价于 Σ; 所以存在矩阵 P, Q 为初等矩阵的乘积, 使得:

$$Q\Gamma P = \Sigma = \mathrm{diag}(\sigma_1, \cdots, \sigma_n).$$

因此, $\Gamma = Q^{-1}\Sigma P^{-1}$. 因为初等矩阵的逆也是初等矩阵, 故 Q^{-1}, P^{-1} 也是初等矩阵的乘积. 因为 Σ 可逆, $\det(\Sigma) = \sigma_1 \cdots \sigma_n$ 为 R 中单位, 故每个 σ_i 是单位, 所以 Σ 是初等矩阵的乘积.

(2) 如果 Γ, Γ' 是 Gauss 等价的, 那么它们总是 R-等价的. 因为如果 $\Gamma' = Q\Gamma P$, 其中 P, Q 为初等矩阵的乘积, 则 P, Q 是可逆的. 相反地, 如果 Γ', Γ 是 $R-$ 等价的, 则 $\Gamma' = Q\Gamma P$, 其中 P, Q 可逆. (1) 中表明 Γ', Γ 是 Gauss 等价的.

□

定理 4.7.17 (相联基 (Simultaneous Bases)). *设 R 为 Euclid 环 F 为有限生成自由 R-模, S 为 F 子模. 则存在 F 的一个基 $z_1, \cdots, z_n$ 与 R 中非零数 $\sigma_1, \cdots, \sigma_q$, 其中 $0 \leq q \leq n$, 使得 $\sigma_1 | \cdots | \sigma_q$, 且 $\sigma_1 z_1, \cdots, \sigma_q z_q$ 为 S 的一个基.*

证明. 如果 $M = F/S$, 则 S 的秩小于 n, 所以:

$$0 \longrightarrow S \xrightarrow{\lambda} F \longrightarrow M \longrightarrow 0$$

为 M 的一个表示, 其中 λ 为嵌入. 现在任意选取 S, F 的基对应 λ 的一个表示矩阵 Γ. 则存在 S, F 的另一个基 X, Y 对应 $\Gamma = {}_Y[\lambda]_X$ 与 Smith 正规型 R-等价. 而这组基就是定理中所说的基. □

推论 4.7.18. *设 R 是 Euclid 环, Γ 为 R-映射 $\lambda : R^t \to R^n$ 在某个基下的表示矩阵, $M = \operatorname{Coker}\lambda$.*

(1) 如果 Γ 与 Smith 正规型 $\operatorname{diag}(\sigma_1, \cdots, \sigma_q) \oplus 0$ R-等价, 则不是单位的 $\sigma_1, \cdots, \sigma_q$ 是 M 的不变因子.

(2) 如果 $\operatorname{diag}(\eta_1, \cdots, \eta_s) \oplus 0$ 为 Γ 的另一 Smith 正规型, 则 $s = q$ 且对于任意的 i 存在单位 u_i 使得 $\eta_i = u_i\sigma_i$, 即对角元是相伴的.

证明. (1) 如果 $\operatorname{diag}(\sigma_1, \cdots, \sigma_q) \oplus 0$ 为 Γ 的 Smith 正规型, 则存在 R^t 的基 $y_1, \cdots, y_t$ 与 R^n 的基 $z_1, \cdots, z_n$ 使得 $\lambda(y_1) = \sigma_1 z_1, \cdots, \lambda(y_q) = \sigma_q z_q$, 且当 $j > q$ 时,$\lambda(y_j) = 0$. 现在 $R/(0) \cong R$ 且当 u 是单位时, $R/(u) = \{0\}$. 如果 σ_s 是第一个不为单位的 σ_i, 则

$$M \cong R^{n-q} \oplus \frac{R}{(\sigma_s)} \oplus \cdots \oplus \frac{R}{(\sigma_q)},$$

为循环模的直和, 其中 $\sigma_s | \cdots | \sigma_q$. 基本定理证明了 $\sigma_s, \cdots, \sigma_q$ 为 M 的不变因子.

(2) 由 (1) 即可得.

□

定理 4.7.19. *域 k 上的两个 n 阶矩阵 A, B 相似当且仅当 $xI - A, xI - B$ 在 $k[x]$ 上有相同的 Smith 正规型.*

证明. A, B 相似当且仅当 $xI - A, xI - B$ 是 $k[x]-$ 等价, 而 $k[x]$ 是 Euclid 环, 故当且仅当有相同的 Smith 正规型. □

推论 4.7.20. *设 F 是有限生成的自由 Abel 群, S 是 F 具有有限指标的子群. 设 $y_1, \cdots, y_n$ 是 F 的一个基, $z_1, \cdots, z_n$ 是 S 的一个基. 设 $A = [a_{ij}]$ 是 n 阶矩阵满足 $z_i = \sum_j a_{ji} y_j$. 则*

$$[F : S] = \mid \det(A) \mid .$$

证明. 改变 S, F 的基, 用与 A 是 $\mathbb{Z}$-等价的矩阵 B 代替 A:

$$B = QAP,$$

其中 Q, P 是 $\mathbb{Z}$ 上的可逆矩阵. 因 $\mathbb{Z}$ 中的单位仅有 1 和-1, 故 $\mid \det(B) \mid = \mid \det(A) \mid$. 特别地. 如果我们选取 B 为 Simth 正规型, 则 $B = \mathrm{diag}(g_1, \cdots, g_n)$, 所以 $|\det(B)| = g_1 \cdots g_n$. 而 $g_1, \cdots, g_n$ 是 F/S 的不变因子, 它们的积为 F/S 的序, 其指标为 $[F : S]$. □

下面讨论的是多项式环 $k[x]$ 中的情景.

定理 4.7.21. *设 $\Gamma = \mathrm{diag}(\sigma_1, \cdots, \sigma_q)$ 是 Euclid 环 R 上的矩阵 Γ 的 Simth 正规型中的对角块. 用归纳的方法定义 $d_i(\Gamma)$:$d_0(\Gamma) = 1$, 对于 $i > 0$,*

$$d_i(\Gamma) = \gcd(\Gamma\text{的所有 } i \text{ 阶子式})$$

则对于任意的 $i \geq 1$,

$$\sigma_i = d_i(\Gamma)/d_{i-1}(\Gamma).$$

证明. 记 $a \sim b$ 为 a, b 在 R 中相伴. 下面证明如果 Γ, Γ' 是 $R-$ 等价的, 则对于所有的 i,

$$d_i(\Gamma) \sim d_i(\Gamma').$$

这样就可以证明定理, 因为如果 Γ' 是 Γ 的 smith 正规型, Γ 的对角块为 $\mathrm{diag}(\sigma_1, \cdots, \sigma_q)$, 则 $d_i(\Gamma') = \sigma_1 \sigma_2 \cdots \sigma_i$. 因此,

$$\sigma_i(x) = d_i(\Gamma')/d_{i-1}(\Gamma') \sim d_i(\Gamma)/d_{i-1}(\Gamma).$$

我们需要证明:

$$d_i(\Gamma) \sim d_i(L\Gamma), d_i(\Gamma) \sim d_i(\Gamma L)$$

对于任意初等矩阵 L 都成立. 事实上, 我们只需证明 $d_i(\Gamma L) \sim d_i(\Gamma)$, 因为:

$$d_i(\Gamma L) = d_i([\Gamma L]^T) = d_i(L^T \Gamma^T)$$

作为最后的简化, 我们只需要考虑第 I,II 类初等变换, 因为我们已经说明第 III 类初等变换可由前两类表示. L 为第一类初等矩阵: 如果我们将 Γ 的 ROW(l) 乘上一个单位 u, 则其 i 阶子矩阵或者不变, 或者其某一行也乘上 u. 在第一种情况中, 其行列式不变. 在第二种情况中, 其行列式乘 u. 因此 $L\Gamma$ 的每个 i 阶子式都是 Γ 对应子式的相伴元, 所以 $d_i(L\Gamma) \sim d_i(\Gamma)$. L 为第二类初等矩阵: 如果用 L 的 ROW(l) + r ROW(j) 代替其 ROW(l), 则 Γ 只有 ROW(l) 改变. 因此 Γ 的 i 阶子矩阵或者没有此行, 或者有. 在第一种情况中, $L\Gamma$ 的对应子式不变. 第二种情况中又有两种子情况:i 阶子矩阵有 ROW(j) 或者没有. 如果其有 ROW(j), 其行列式不变. 如果子矩阵不含 ROW(j), 则新的子式形式为 $m + rm'$, 其中 m, m' 为 Γ 的 i 阶子式. 所以 $d_i(\Gamma)|d_i(L\Gamma)$, 因为 $d_i(\Gamma)|m, d_i(\Gamma)|m'$. 因为 L^{-1} 也是第二类初等矩阵, 以上讨论也证明了 $d_i(L\Gamma)|d_i(L^{-1}(L\Gamma))$. 而,

$$L^{-1}(L\Gamma) = \Gamma$$

故 $d_i(\Gamma), d_i(L\Gamma)$ 互相整除. 又因为 R 是整环, 所以 $d_i(L\Gamma) \sim d_i(\Gamma)$. □

定理 4.7.22. *存在计算域 k 上任意方阵 A 初等因子的算法.*

证明. 我们只需要找到 $\Gamma = xI - A$ 在环 $k[x]$ 上的 Smith 正规型, 则 A 的不变因子就是其中非零非单位的对角元素. 我们有两种算法:

(1) 对于所有的 i, 计算出 $d_i(xI - A)$.

(2) 通过 $k[x]$ 上的 Gauss 消元法计算 $xI - A$ 的 Smith 正规型.

□

例 4.7.23. 计算矩阵

$$A = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 1 \\ 0 & 0 & -4 \end{bmatrix}$$

在 $\mathbb{Q}$ 中的不变因子. 我们将使用两种方法的结合来计算. 现在:

$$xI - A = \begin{bmatrix} x-2 & -3 & -1 \\ -1 & x-2 & -1 \\ 0 & 0 & x+4 \end{bmatrix}.$$

显然 $g_1 = 1$. 交换 ROW(1), ROW(2) 并改变第一行的符号得到

$$\begin{bmatrix} 1 & -x+2 & 1 \\ x-2 & -3 & -1 \\ 0 & 0 & x+4 \end{bmatrix}.$$

将 ROW(2) 加上 $-(x-2)\,\mathrm{ROW}(1)$ 得到

$$\begin{bmatrix} 1 & -x+2 & 1 \\ 0 & x^2-4x+1 & -x+1 \\ 0 & 0 & x+4 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & x^2-4x+1 & -x+1 \\ 0 & 0 & x+4 \end{bmatrix}.$$

因子矩阵

$$\begin{bmatrix} x^2-4x+1 & -x+1 \\ 0 & x+4 \end{bmatrix}$$

中元素的最大公因数为 1, 故 $g_2 = 1$. 所以 A 只有一个不变因子, 即 $(x^2-4x+1)(x+4) = x^3-15x+4$, 且其必为 A 的特征多项式. 特别地, 其有理标准型为:

$$\begin{bmatrix} 0 & 0 & -4 \\ 1 & 0 & 15 \\ 0 & 1 & 0 \end{bmatrix}.$$

例 4.7.24. Abel 群 G 有生成元 a, b, c 和关系

$$\begin{aligned} 7a+5b+2c &= 0, \\ 3a+3b &= 0, \\ 13a+11b+2c &= 0. \end{aligned}$$

通过 $\mathbb{Z}$ 上的初等变换, 我们可以得到关系矩阵的 Smith 正规型:

$$\begin{bmatrix} 7 & 5 & 2 \\ 3 & 3 & 0 \\ 13 & 11 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

所以 $G \cong (\mathbb{Z}/1\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \bigoplus (\mathbb{Z}/0\mathbb{Z})$, 即 $G \cong \mathbb{Z}_6 \oplus \mathbb{Z}$.

第五章　有限群的结构理论

5.1　群作用

(1) 主要回顾一下群作用的定义与例子, 了解和掌握子群在 G 的陪集的表示, 同时会有稳定子群 (化子), 中心化子, 轨道, 正规化子以及 $p-$ 群的出现.

(2) 证明一些关于群作用与 $p-$ 群的定理, 包括 Caley 定理, Cauchy 定理 $N\backslash C$ 定理等以及一些命题和推论的证明.

定理 5.1.1. ***(Caley 定理)*** *每个群 G 都同构于对称群 S_G 的一个子群 (特别地, 若 $|G|=n$, 则 G 同构于 S_n 的一个子群).*

证明. 对于每个 $a\in G$, 定义' 平移':

$$\begin{aligned}\tau_a : G &\to G\\ x &\mapsto \tau_a(x)=ax\end{aligned}$$

若 $a\neq 1$, 则 τ_a 不是同态. 因为 $\tau_a(x_1x_2)=ax_1x_2\neq \tau_a(x_1)\tau_a(x_2)$. 对 $a,b\in G$, 有结合性:

$$(\tau_a\circ\tau_b)(x)=\tau_a(\tau_b(x))=\tau_a(bx)=a(bx)=(ab)x$$

故 $\tau_a\circ\tau_b=\tau_{ab}$, 则 τ_a 的逆为 $\tau_{a^{-1}}$, 所以每个 τ_a 都是双射, 于是 $\tau_a\in S_G$. 定义:

$$\begin{aligned}\phi : G &\to S_G\\ a &\mapsto \phi(a)=\tau_a\end{aligned}$$

于是, $\phi(a)\phi(b)=\tau_a\tau_b=\tau_{ab}=\phi(ab)$, 故 ϕ 为同态. 又若 $\phi(a)=\phi(b)$, 则 $\tau_a=\tau_b$, 此时对任意 $x\in G$, $\tau_a(x)=\tau_b(x)$(当 $x=1$ 时, $a=b$), 故 ϕ 为单射. 又 ϕ 显然是满的, 故 ϕ 为同构. 又有结论: 若 x 是满足 $|x|=n$ 的集合, 则 $s_x\cong S_n$. 从而定理得证. □

定理 5.1.2. ***(陪集上的表示)*** *设 G 为群, H 是 G 的有限指数 n 的子群, 则存在同态 $\phi: G\longrightarrow S_n$ 使得 $\operatorname{Ker}\phi\leq H$.*

证明. 即使 H 可能不是 G 中的正规子群, 仍然可记 H 在 G 中的一切陪集的族 G/H. 对每个 $a \in G$, 定义' 平移':

$$\begin{aligned} \tau_a : G/H &\to G/H \\ x &\mapsto \tau_a(xH) = axH \end{aligned}$$

对 $a, b \in G$, 由结合性:

$$(\tau_a\tau_b)(xH) = \tau_a(\tau_b(xH)) = \tau_a(bxH) = a(bxH) = (ab)xH$$

于是, $\tau_a\tau_b = \tau_{ab}$. 同理 $\tau_a^{-1} = \tau_{a^{-1}}$. 也同理可证 τ_a 是双射 (任意 $a \in G$). 从而 $\tau_a \in S_{G/H}$, 定义:

$$\begin{aligned} \phi : G &\to S_{G/H} \\ a &\mapsto \phi(a) = \tau_a \end{aligned}$$

于是有 $\phi(a)\phi(b) = \tau_a\tau_b = \phi(ab)$. 故 ϕ 为同态, 又若 $a \in \operatorname{Ker}\phi$, 则 $\phi(a) = 1_{G/H}$, 因此对于任意的 $x \in G$, $\tau_a(xH) = xH$. 特别地, 当 $x = 1$ 时, $aH = H$. 注意到, 若 H 时 G 的子群, 且 $a, b \in G$, 则 $aH = bH$ 当且仅当 $b_{-1}a \in H$). 故 $a \in H$. 又因 $| G/H | = n$, 则 $S_{G/H} \simeq S_n$. 特别地, 当 $H = 1$ 时, $S_g \simeq S_n$. □

定义 5.1.3. 设 G 是一个群, X 为一个非空集合. 若映射 f 满足:

$$f : G \times X \longrightarrow X$$

(1) $f(e, x) = x$, 对任意 $x \in X$.

(2) $f(g_1g_2, x) = f(g_1, f(g_2))$, 对任意 $g_1, g_2 \in G, x \in X$.

称 f 决定了**群 G 在集合 X 上的作用 (actions of group on set)**. 通常将 $f(g, x)$ 记为 $(g.x)$, 故 $(e, x) = x$; $(g_1g_2).x = g_1.(g_2.x)$.

由定义知, 若群 G 作用在集合 X 上, 则 G 中的每个元素 g, 均对应于集合 X 到自身的一个映射 $\sigma(g)$:

$$\begin{aligned} \sigma_g : X &\to X, \\ x &\mapsto (g.x) \end{aligned}$$

注意到:

$$g^{-1}.(g.x) = (g^{-1}g).x = e.x = x = (gg^{-1}).x = g.(g^{-1}.x)$$

所以 $\sigma \in S(x)$, 且 $\sigma_g^{-1} = \sigma_{g^{-1}}$. 从而 $\varphi : g \to \sigma_g$ 是从群 G 到 $S(x)$ 的一个同态. 反过来, 若 $\psi : G \to S(x)$ 是一个群同态, 则可定义:

$$g.x := \psi(g)(x), g \in G, x \in X$$

由此决定了群 G 在集合 X 上的一个作用. $e.x = x$; 且满足结合性:

$$g_1.(g_2.x) = g_1(\psi(g_2)(x)) = \psi(g_1)(\psi(g_2)(x)) = \psi(g_1g_2)x = (g_1g_2).x$$

例 5.1.4. (1) 左平移作用:

$$\begin{aligned} G \times G &\to G \\ (g.x) &\mapsto gx \end{aligned}$$

(2) 右平移作用:

$$\begin{aligned} G \times G &\to G \\ (g.x) &\mapsto xg^{-1} \end{aligned}$$

(3) 群上的共轭作用:

$$\begin{aligned} G \times G &\to G \\ (g.x) &\mapsto gxg^{-1} \end{aligned}$$

(4) 子群上的共轭作用: $H \leq G, X = \{xH \mid x \in G\}$ 则:

$$\begin{aligned} G \times X &\to X \\ (g.xH) &\mapsto gxH \end{aligned}$$

例 5.1.5. 可证明 G 由共轭作用在它自身上, 即对每个 $g \in G$, 定义:

$$\begin{aligned} a_g : G &\to G \\ g &\mapsto a_g(x) = gxg^{-1} \end{aligned}$$

证明. 验证公理 (1): 对任意的 g, 有 $a_1(g) = 1x1^{-1} = x$, 故 $a_1 = 1_G$. 验证公理 (2): 对任意 $x \in G$,

$$(a_ga_h)(x) = a_(g(a_h(x))) = a_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = a_{gh}(x)$$

故 $a_g \circ a_h = a_{gh}$. □

定义 5.1.6. 设群 G 作用在集合 X 上, 从而我们得到从 G 到 S_x 的一个群同态. 若该同态为单射, 则称 G 在 X 作用上是**忠实的 (faithful)**. 设 X, X' 是两个非空集合, 且 G 同时作用在 X 与 X' 上. 若存在双射:

$$\begin{aligned} \phi : X &\to X' \\ x &\mapsto \phi(g.x) = g.\phi(x) \end{aligned}$$

则称这个作用是**等价的 (equivalent)**.

例 5.1.7. 左平移作用与右平移作用是等价的.

$$\begin{aligned}\phi : G &\to G\\ x &\mapsto x^{-1}\end{aligned}$$

而容易计算 $\phi(g.x) = \phi(gx) = (gx)^{-1} = x^{-1}g^{-1}$.

定义 5.1.8. 设群 G 作用在非空集合 X 上, 任意 $x, y \in X$, 若存在 $g \in G$ 使得 $y = g.x$; 则称 x 与 y 等价, 记为 $x \sim y$. 此时 X 被划分成一些等价类的并, 每一个等价类称为一个**轨道 (orbit)**.

注 56. 包含 x 的轨道记为 $\mathrm{O}_x = \{g.x \mid g \in G\}$. 而因为群作用给出了集合 X 上的一个划分, 从而 X 是一些不交的轨道并. $X = \sqcup_x \mathrm{O}_x$. O_x 可能只有一个元素 x, 此时任取 $g \in G$ 有 $g.x = x$, 这样的元素称为**不动元素 (fixed piont)**.

例 5.1.9. (1)

$$\begin{aligned}G \times G &\to G\\ (g.x) &\mapsto gxg^{-1}\end{aligned}$$

若 $x \in \mathrm{C}_G$, 则 $\mathrm{O}_x = \{x\}$; 同样的, 若 $\mathrm{O}_x = \{x\}$, 则 $x \in C_G$. 若 x 只有一个轨道, 则称群 G 在 x 上的作用是**传递的 (transitive)**, 此时如果任取 $x, y \in G$, 存在 $g \in G$ 使得 $y = g.x$.

(2) 设 V 是一个 n 维实向量空间, 令 $X = V/\{0\}$, 则左平移作用是传递的:

$$\begin{aligned}\mathrm{GL}_n(R) \times X &\to X\\ (A, x) &\mapsto Ax\end{aligned}$$

定义 5.1.10. 任取 $x \in X$, 令 $\mathrm{Stab}_G(x) := \{g \in G \mid g.x = x\}$, 则 $Stab_G(x) \leq G$, 称为 x 的**稳定子群 (stablizer)**.

定理 5.1.11 (群在轨道上作用与群在稳定化子上作用等价). *若群 G 作用在集合 X 上, $x \in G$, 记 O_x 为集合 X 中含有 x 的轨道, $\mathrm{Stab}_G(x)$ 为 x 的稳定子群, 则 G 在集合 O_x 上的作用与 G 在 $G/\mathrm{Stab}_G(x)$ 上的作用等价.*

证明. G 在 O_x 上的作用为:

$$\begin{aligned}G \times \mathrm{O}_x &\to \mathrm{O}_x\\ (g.y) &\mapsto g.y\end{aligned}$$

任取 $a\,\mathrm{Stab}_G(x) \in G/\mathrm{Stab}_G(x)$; 对任意 $g \in a\,\mathrm{Stab}_G(x)$, 有 $g.x = a.x$. (即同一个陪集中, 不同元素将 x 变到同一个元素). 反之, 若 $g_1, g_2 \in G$, 且 $g_1.x = g_2.x$. 则

$(g_2^{-1}g_1).x = x$, 从而 $g_2^{-1}g_1 \in \mathrm{Stab}_G(x)$, 进而 $g_1 \in g_2\,\mathrm{Stab}_G(x)$, 所以 g_1, g_2 属于同一个左陪集. 定义:

$$\Psi : G/\,\mathrm{Stab}_G(x) \to \mathrm{O}(x)$$

$$g\,\mathrm{Stab}_G(x) \mapsto g.x$$

从而 Ψ 是一个一一对应. 因为 $\mathrm{Ker}(\Psi) = \mathrm{Stab}_G(x)$, 从而 Ψ 是单射. 又任意 $g.x \in O_x$, 存在 $g\,\mathrm{Stab}_G(x) \in G/\,\mathrm{Stab}_G(x)$ 使得 $\Psi(g\,\mathrm{Stab}_G(x)) = g.x$, 于是 Ψ 是满射. 又注意到:

$$\Psi(g', g\,\mathrm{Stab}_G(x)) = g'.(g.x) = g'.\Psi(g\,\mathrm{Stab}_G(x))$$

综上定理得证. □

推论 5.1.12. *设 G 是有限群, G 作用在集合 X 上, 则 X 中的任意一个轨道 O_x 包含有限多的元素, 且 $|\,\mathrm{O}_x\,| = [G : \mathrm{Stab}_G(x)]$.*

证明. 任取 $x \in G$, 设 $Stab_G(x)$ 是 x 的稳定子群, 则由轨道—稳定子定理(5.1.13)得, $|\,\mathrm{O}_x\,| = [G : \mathrm{Stab}_G(x)]$. □

定理 5.1.13 (轨道—稳定子定理). *若群 G 作用在 X 上且 $x \in X$, 则 $|\,\mathrm{O}_x\,| = [G : G_x]$ 是 G 中的稳定化子 G_x 的指数.*

证明. 令 G/G_x 为 G 中 G_x 的一切左陪集的族, 又因为 $|\,G/G_x\,| = [G : G_x]$, 于是我们列出一个双射:

$$\phi : G/G_x \to \mathrm{O}_x$$

$$\phi : gG_x \mapsto gx$$

ϕ 的定义是合理的. ϕ 是单的: 若 $gx = \phi(gG_x) = \phi(hG_x) = hx$, 则 $h^{-1}gx = x$, 因此 $h^{-1}g \in G_x$, 从而 $gG_x = hG_x$. ϕ 是满的: 若 $y \in \mathrm{O}_x$, 则有某个 $g \in G$ 使得 $y = gx$, 从而 $y = \phi(gG_x)$. 故 ϕ 是双射, 从而有 $_x\,| = [G : G_x] =|\, G/G_x\,|$. □

性质 5.1.14. *若 G 作用在集合 X 上, 则 X 是轨道的不相交并, 若 X 是有限的, 则 $|\,X\,| = \sum_i |\,O_{x_i}\,|$, 其中从每个轨道中选一个 x_i.*

推论 5.1.15. *设 p 为一个素数, G 是有限群. 若 $|\,G\,| = p^k (k \geq 1)$, 则称 G 为一个$p-$* ***群 (p—group)****. 设 G 是一个 $p-$ 群, 且该群作用在有限集 X 上, 且若 $|\,X\,| = n, (n, p) = 1$, 则 X 中必有不动元素.*

证明. 设 $\mathrm{O}_{x_1}, \mathrm{O}_{x_2}, \cdots, \mathrm{O}_{x_m}$ 为 X 中的所有轨道, x_i 是不动元素, 则 $|\,\mathrm{O}_{x_i}\,| = 1$, 由推论(5.1.15), 若 x_i 不是不动元素, 则:

$$|\,O_{x_i}\,| = p^k (l \geq 1)$$

而 $X = \sqcup_{i=1}^{m} \mathrm{O}_{x_i}$, 于是 $\mid X \mid = \sum_{i=1}^{m} \mid \mathrm{O}_i \mid$. 所以 $n = \sum_{i=1}^{m} \mid \mathrm{O}_{x_i} \mid$. 又因 $\gcd(n,p) = 1$, 所以必有 x_i 使得 $\mid \mathrm{O}_i \mid = 1$. 否则, 有 $\mid \mathrm{O}_{x_i} \mid\mid G \mid = p^l$, 从而有 $\mid \mathrm{O}_{x_i} \mid = p^{l_i}$. 故 $\gcd(n,p) \neq 1$, 矛盾. 得证. □

推论 5.1.16. *设 G 是一个 $p-$ 群, G 作用在一个有限集 X 上, 且假设 $\mid x \mid = n$. 若 t 为 X 中的不动元素的个数, 则 $t \equiv n \pmod{p}$.*

证明. 由

$$n = t + \sum_{|O_x| \geq 1} \mid O_x \mid$$

可得. □

推论 5.1.17. *$p-$ 群必有非平凡的中心.*

证明. 设 G 是一个 $p-$ 群, 考虑 G 到 G 的作用为共轭变换; 此时, 只有中心元素才构成单个元素的轨道. 令 $t = \mid C_G \mid$, 则知 $t \geq 1$. 又推论(5.1.17)知:

$$t \equiv \mid G \mid \pmod{p} t \equiv 0 \pmod{p} \Rightarrow t \geq 1$$

□

注 57. 当群 G 作用在 (共轭作用) 在群 G 上时, 包含 G 中元素 x 的轨道称为 x 所在的共轭类, 记为 $\mathrm{C}(x)$. 若 $\mid G \mid < \infty$. 则 $\mid \mathrm{C}(x) \mid = [G : \mathrm{Stab}_G(x)]$. 此时,

$$\mathrm{Stab}_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$$

记 $\mathrm{Z}(x) = \mathrm{Stab}_G(x)$, 称为 x 的**中心化子 (centralizer)**.

$$\mathrm{Z}(x) = G \Longleftrightarrow x \in \mathrm{C}_G(x)$$

若 $\mid G \mid < \infty$, 则

$$\mid G \mid = \mid \mathrm{C}_G(x) \mid + \sum_{x} [G : \mathrm{Z}(x)]$$

定理 5.1.18. ***(Cauchy 定理)*** *G 是有限群, 素数 p 满足 $p \mid\mid G \mid$, 则 G 含有 p 阶元素.*

证明. 对 $m \geq 1$ 用数学归纳法证明该定理, 其中 $\mid G \mid = pm$. 由 Largrange 定理证明在 p 阶群中每个非幺元元素的阶都是 p, 故 $m = 1$ 为真. 现进行归纳, 若 $x \in G$, 则 x 的共轭个数是 $\mid x^G \mid = [G : \mathrm{C}_G(x)]$, 其中 $\mathrm{C}_G(x)$ 是 x 在 G 中的中心化子. 注意到, 若 $x \notin \mathrm{Z}(G)$, 则 x^G 的元素多于一个, 因此 $\mid \mathrm{C}_G(x) \mid < \mid G \mid$. 若对某个非中心的 x, $p \mid\mid \mathrm{C}_G(x) \mid$, 则根据归纳假设得, 在 $C_G(x) \leq G$ 中有 p 阶元素, 从而得证. 故假定, 对一切的非中心元素 $x \in G$, $p \nmid \mathrm{C}_G(x) \mid$, 因 p 是素数且 $\mid G \mid = [G : \mathrm{C}_G(x)] \mid \mathrm{C}_g(x) \mid$, 根据由 Euclid 引理:

$$p \mid [G : \mathrm{C}_G(x)]$$

注意到, $\mathrm{Z}(G)$ 由一切满足 $\mid x^G \mid = 1$ 的元素 $x \in G$ 组成. 由类方程:

$$\mid G \mid = \mid Z(G) \mid + \sum_i [G : C_G(x)]$$

其中, 在每个多于一个元素的共轭类中挑出一个元素 x_i, 因 $\mid G \mid$ 和 $[G : \mathrm{C}_G(x)]$ 都被 p 整除, 从而 $\mid \mathrm{Z}(G) \mid$ 被 p 整除, 但 $\mathrm{Z}(G) = C_G(G)$ 为 Abel 群. 根据 G 是有限 Abel 群, d 是 $\mid G \mid$ 的因数, 则 G 有 d 阶子群. 从而, $\mathrm{Z}(G)$ 含 p 阶元素, 即 G 包含 p 阶子群. □

定理 5.1.19. ***(N/C 引理)***

(1) 若 $H \leq G$, 则 $\mathrm{C}_G(H) \lhd \mathrm{N}_G(H)$, 并且有一个单射

$$\mathrm{N}_G(H)/\mathrm{C}_G(H) \hookrightarrow \mathrm{Aut}(H)$$

(2) $G/\mathrm{Z}(G) \simeq \mathrm{Inn}(G)$, 其中 $\mathrm{Inn}(G)$ 是 $\mathrm{Aut}(G)$ 中所有包含内自同构的子群.

证明. (1) 因为 $H \lhd \mathrm{N}_G(H)$, 故 $nhn^{-1} = h'$, 即 $nh = h'n$. 又 $H \lhd \mathrm{C}_G(H)$, 故 $hc = ch$, 即 $c = hch^{-1}$. 所以:

$$\begin{aligned} ncn^{-1} = n(hch^{-1})n^{-1} &= (nh)c(nh)^{-1} \\ &= (h'n)c(h'n)^{-1} \\ &= h'ncn^{-1}h'^{-1} \\ &= h'(ncn^{-1})h'^{-1} \end{aligned}$$

于是, 有 $h'(ncn^{-1}) = (ncn^{-1})h'$, 故 $ncn^{-1} \in \mathrm{C}_G(H)$. 即 $\mathrm{C}_G(H) \lhd \mathrm{N}_G(H)$. 而对于 $n \in \mathrm{N}_G(H)$ 有共轭变换 $\sigma_n : h \to nhn^{-1}$. 构建同态:

$$\begin{aligned} \tau : N_G(H) &\to Aut(H) \\ n &\mapsto \sigma(n) \end{aligned}$$

于是, $\mathrm{Ker}(\tau) = \{n \in \mathrm{N}_G(H) \mid \sigma_n(h) = nhn^{-1} = h\} = \mathrm{C}_G(H)$. 则由第一同态定理有:

$$\mathrm{N}_G(H)/\mathrm{C}_G(H) \simeq \tau(\mathrm{N}_G(H))$$

又 $\tau(N_G(H)) \leqslant \mathrm{Aut}(H)$, 故有 $\mathrm{N}_G(H)/\mathrm{C}_G(H) \hookrightarrow \mathrm{Aut}(H)$.

(2) 当 $H = G$ 时, 则有 $\mathrm{N}_G(H) = G$, $\mathrm{C}_G(H) = \mathrm{Z}(G)$ 且 $\mathrm{Im}(\phi) = \mathrm{Im}(H) = \mathrm{Im}(G)$, 故命题得证.

□

5.2 Sylow 定理

本次讨论班我们首先将介绍 Sylow p-子群, 证明 Sylow 定理, 并探究 Sylow p-子群与正规子群的联系, 进而证明阶小于 60 的非 Abel 群 G 不是单群, 最后我们将给出一些 p-群新例.

定义 5.2.1 (**Sylow p-子群**). 设 p 是素数. 有限群 G 的 Sylow p-子群是极大 p-子群 P.

引理 5.2.2. *设 P 是有限群 G 的一个 Sylow p-子群*

(1) P 的每个共轭也是 G 的 Sylow p-子群.

(2) $|N_G(P)/P|$ 与 p 互素.

(3) 如果 $a \in G$ 的阶为 p 的某个幂且 $aPa^{-1} = P$, 则 $a \in P$.

证明. (1) 如果 $a \in G$, 则 aPa^{-1} 是 G 的 p-子群. 如果它不是极大 p-子群, 则存在 p-子群 Q 使得 $aPa^{-1} \leqslant Q$. 因此 $P \leqslant a^{-1}Qa$, 矛盾.

(2) 如果 p 整除 $|N_G(P)/P|$, 则由 Cauchy 定理(5.1.18)可知 $N_G(P)/P$ 包含 p 阶元素 aP, 因此 $N_G(P)/P$ 包含 p 阶子群 $S^* = \langle aP \rangle$. 由对应定理可知, 存在 S, 使得 $P \leq S \leq N_G(P)$, 且 $S/P \cong S^*$. 而 S 是 $N_G(P) \leq G$ 的 p-子群, 它严格地大于 P, 与 P 的极大性矛盾. 由此可知 p 不整除 $|N_G(P)/P|$.

(3) 由正规化子定义可知, $a \in N_G(P)$. 若 $a \notin P$, 则陪集 aP 是 $N_G(P)/P$ 的非平凡元素, 其阶为 p 的某个幂, 依据上一条, 与 Lagrange 定理矛盾.

□

注 58. (1) 设 G 是有限群, p 是素数, H 是 G 的正规子群. 若 $|H|$ 和 $|G/H|$ 两者都是 p 的幂, 则 $|G|$ 也是 p 的幂.

(2) 由于 Sylow p-子群的每个共轭也是 Sylow p-子群, 所以令 G 用共轭作用在 Sylow p-子群上是合理的.

定理 5.2.3 (**Sylow**). *设 G 是有限群, 阶为 $p_1^{l_1} \dots p_t^{l_t}$, 并设 P 是 G 的 Sylow p-子群, 其中 p 是某个素数 $p = p_j$.*

(1) 每个 Sylow p-子群都与 P 共轭.

(2) 如果存在 r_j 个 Sylow p_j-子群, 则 r_j 是 $|G|/p_j^{l_j}$ 的因数, 且:

$$r_j \equiv 1 \operatorname{Mod} p_j$$

证明. 设 $X = \{P_1, \dots P_{r_j}\}$ 是 P 一切共轭的集合, 其中, 记 P 为 P_1. 若 Q 是 G 的一个 Sylow p-子群, 则将 Q 共轭作用在 X 上, 即:

若 $a \in Q$, 则有

$$P_i = g_i P g_i^{-1} \mapsto a(g_i P g_i^{-1})a^{-1} = (ag_i)P(ag_i)^{-1} \in X.$$

由于任一轨道中的元素个数是 $|Q|$ 的因数, 且 Q 为 p-群, 则每个轨道的大小为 p 的某个幂. 如果有一个轨道的大小为 1, 则存在某个 P_i 使得对一切 $a \in Q$,$aP_ia^{-1} = P_i$. 根据引理, 对一切 $a \in Q$ 有 $a \in P_i$, 则 $Q \leq P_i$. 而 Q 为一个 Sylow p-子群, 它是 G 的极大 p-子群, 从而 $Q = P_i$. 特别地, 如果 $Q = P_1$, 则只有一个大小为 1 的轨道, 它就是 $\{P_1\}$, 其他一切轨道的大小都是 p 的真正的幂. 由此可知, $|X| = r_j \equiv 1 \,\mathrm{Mod}\, p_j$.

假设存在某个 Sylow p-子群 Q, 它不是 P 的共轭, 即对任意 i,$Q \neq P_i$. 我们令 Q 作用在 X 上, 若有大小为 1 的轨道, 如 $\{P_k\}$, 则有 $Q = P_k$, 与假设矛盾. 因此, 没有大小为 1 的轨道, 这就是说每个轨道的大小都是 p 真正的幂, 因此 $|X| = r_j$ 是 p 的倍数, 即 $r_j \equiv 0 \,\mathrm{Mod}\, p$. 与 $r_j \equiv 1 \,\mathrm{Mod}\, p$ 矛盾, 则 Q 不存在.

由于一切 Sylow$p$-子群共轭, 所以有 $r_j = [G : N_G(P)]$, 从而 r_j 是 $|G|$ 的因数. 而 $r_j \equiv 1 \,\mathrm{Mod}\, p_j$, 所以由 Euclid 引理得. $r_j \,||\, G \,|\, /p_j^{l_j}$. □

推论 5.2.4. *有限群 G 对某个素数 p 有唯一的 Sylow$p$-子群 P, 当且仅当 $P \lhd G$.*

证明. 假定 G 的 Sylow p-子群 P 是唯一的. 对每个 $a \in G$, 共轭 aPa^{-1} 也是 Sylow p-子群. 由于唯一性, 对一切 $a \in G$,$aPa^{-1} = P$, 从而 $P \lhd G$.

反之, 假设 $P \lhd G$. 如果 Q 是任一 Sylow p-子群, 则对某个 $a \in G$ 有 $Q = aPa^{-1}$. 但由正规性, $aPa^{-1} = P$, 所以 $Q = P$. □

定理 5.2.5 (Sylow). *如果 G 是 p^lm 阶有限群, 其中 p 是素数且 $p \nmid m$, 则 G 的每个 Sylow p-子群 P 的阶为 p^l.*

证明. 先证明 $p \nmid [G : P]$. 有

$$[G : P] = [G : N_G(P)][N_G(P) : P]$$

第一个因子 $[G : N_G(P)] = r$ 是 G 中 P 的共轭的个数, 由于 $r \equiv 1 \,\mathrm{Mod}\, p$, 所以 p 不整除 $[G : N_G(P)]$. 第二个因子 $[N_G(P) : P] = |\, N_G(P)/P \,|$, 根据引理, 也不能被 p 整除. 因此, 由 Euclid 引理,p 不能整除 $[G : P]$.

现在有某个 $k \leq l$ 使得 $|P| = p^k$, 从而

$$[G : P] = |\, G \,| \,/\, |\, P \,| = p^lm/p^k = p^{l-k}m.$$

因 p 不整除 $[G : P]$, 则有 $k = l$. □

例 5.2.6. (1) 设 $G = S_4$. 现在 $|S_4| = 24 = 2^33$. 于是 S_4 的一个 Sylow 2-子群的阶为 8. S_4 包含二面体群 D_8 的一个复制. 由 Sylow 定理, 一切 8 阶子群都共轭于 D_8. 此外, Sylow 2-子群的个数 r 是 24 的因数, 对于 $\mathrm{Mod}\, 2$ 同余于 1, 即 r 是 24 的奇因数. 因 $r \neq 1$, 恰有 3 个 Sylow2-子群.

(2) 如果 G 是有限 Abel 群, 则一个 Sylow p-子群正是它的 p-准素分量; 由于 G 是 Abel 群, 每个子群都是正规子群, 从而对每个素数 p 存在唯一的 Sylow p-子群.

定理 5.2.7. *如果 G 是 $p^l m$ 阶有限群, 其中 p 是素数且 $p \nmid m$, 则 G 有 p^l 阶子群.*

证明. 设 X 是 G 的一切恰有 p^l 个元素的子集的族, 则 $| X | = \binom{p^l m}{p^l}$. 可知 $p \nmid | X |$. 现在 G 作用在 X 上: 对 $g \in G$ 和 $B \in X$, 定义 gB 为

$$gB = \{gb : b \in B\}.$$

如果对每个 $B \in X$, p 整除 $| \mathrm{O}(B) |$, 其中 $\mathrm{O}(B)$ 为 B 的轨道, 则由于 X 是轨道的不相交并, 所以 p 是 $| X |$ 的因数. 由于 $p \nmid | X |$, 因此存在子集 B 满足 $| B | = p^l$ 且 $| \mathrm{O}(B) |$ 不能被 p 整除. 如果 G_B 是这个子集 B 的稳定化子, 则由于 $[G : G_B] = | \mathrm{O}(B) |$, 从而 $| G | = | G_B | \, | \mathrm{O}(B) |$. 因为 $p^l \, || \, | G |$ 且 $p \nmid | \mathrm{O}(B) |$, 则由 Euclid 引理有 $p^l \, || \, | G_B |$. 因此 $p^l \leq | G_B |$. 选择一个元素 $b \in B$ 并定义函数:

$$\begin{aligned} \phi : G_B &\to B \\ g &\mapsto gb \end{aligned}$$

注意, 由于 $g \in G_B$, 其中 G_B 是 B 的稳定化子, 则 $\phi(g) = gb \in gB = B$.. 如果 $g, h \in G_B$ 且 $h \neq g$, 则 $\phi(h) = hb \neq gb = \phi(g)$; 即 ϕ 是单射. 由此可知 $| G_B | \leq | B | = p^l$, 从而 G_B 是 G 的 p^l 阶子群. □

定理 5.2.8 (幂零群的等价刻画). *一切 Sylow 子群都是正规子群的有限群 G 是它的 Sylow 子群的直积.*

证明. 设 $| G | = p_1^{l_1} \dots p_t^{l_t}$, 并设 G_{p_i} 是 G 的 Sylow p_i-子群. 由一切 Sylow 子群生成的子群 S 是 G, 这是由于 $\forall i$, $p_i^{l_i} \, || \, | S |$. 如果 $x \in G_{p_i} \cap \langle \bigcup_{j \neq i} G_{p_j} \rangle$, 则 $x = s_i \in G_{p_i}$, 且 $x = \prod_{j \neq i} s_j$, 其中 $s_j \in G_{p_j}$. 现在对某个 $n \leq 1$ 有 $x^{p_i^n} = 1$. 另一方面, 存在 p_j 的某个幂, 比如 q_j, 使得对一切 j, $s_j^{q_j} = 1$. 由于 s_j 互相可交换, 因此有 $1 = x^q = (\prod_{j \neq i} s_j)^q$, 其中 $q = \prod_{j \neq i} q_j$. 因 $(p_i^n, q) = 1$, 所以存在整数 u 和 v 使得 $1 = up_i^n + vq$, 从而:

$$x = x^1 = x^{up_i^n} x^{vq} = 1$$

所以 G 是它的 Sylow 子群的直积. □

引理 5.2.9. *不存在 $| G | = p^l m$ 阶的非 Abel 单群 G, 其中 p 是素数, $p \nmid m$ 且 $p^l \nmid (m-1)!$.*

证明. 断言: 若 p 是素数, 则每个满足 $| G | > p$ 的 p-群 G 都不是单群. 由于每个有限 p-群有非平凡的中心, 但 $\mathrm{Z}(G) \lhd G$, 则若 $\mathrm{Z}(G)$ 是真子群, 则 G 不是单群. 如果 $\mathrm{Z}(G) = G$,

则 G 是 Abel 群, 则除非 $|G|=p$, 否则 G 不是单群. 假设这样的单群 G 存在. 由 Sylow 定理, G 包含一个 p^l 阶子群 P, 因而它的指数是 m. 因为非 Abel$p$-群不会是单群, 所以可以假定 $m>1$. 由陪集上的表示, 存在同态 $\varphi: G\to S_m$ 使得 $\operatorname{Ker}\varphi\leq P$. 然而 G 是单群, 它没有真正规子群, 因此 $\operatorname{Ker}\varphi=\{1\}$, 从而 φ 是单群, 即 $G\cong\varphi(G)\leq S_m$. 根据 Lagrange 定理, $p^l m\mid m!$, 从而 $p^l\mid(m-1)!$, 与假设矛盾. □

定理 5.2.10. *不存在阶小于 60 的非 Abel 单群.*

证明. 可以验证介于 2 和 59 之间的整数 n, 既不是素数幂也没有引理陈述中的形如 $n=p^l m$ 的因数分解, 这样的 n 有 $30, 40$ 和 56.

下面以证明不存在 30 阶单群为例. 假设存在 30 阶单群 G. 令 P 是 G 的 Sylow 5-子群, 从而 $|P|=5$. P 的共轭的个数 r_5 是 30 的因数且 $r_5\equiv 1 \bmod 5$. 现在 $r_5\neq 1$, 否则 $P\lhd G$, 所以 $r_5=6$. 根据 Lagrange 定理, 这些群的任意两个的交是平凡群. 每个群中有四个非幺元的元素, 则它们的并中有 $6\times 4=24$ 个非幺元元素. 类似地, G 的 Sylow 3-子群的个数 r_3 是 10, 由于 $r_3\neq 1$, 则 r_3 是 30 的因数且 $r_3\equiv 1 \bmod 3$. 每个这种群有两个非幺元的元素, 从而这些群的并中有 20 个非幺元的元素. 我们算出的元素个数已经超过了 G 中的元素的个数, 所以 G 不是单群. □

定理 5.2.11. *设 G 是有限群. 如果 p 是素数且 p^k 整除 $|G|$, 则 G 有 p^k 阶子群.*

证明. 如果 $|G|=p^l m$, 其中 $p\nmid m$, 则 G 的一个 Sylow$p$-子群的阶为 p^l. 因此, 如果 p^k 整除 $|G|$, 则 p^k 整除 $|P|$, 由于 P 有 p^k 阶子群, 则 G 有 p^k 阶子群. □

定义 5.2.12. 域 k 上的**单位上三角矩阵 (unit uppertriangular matrix)** 是指对角线元素为 1 的上三角矩阵. 定义 $\mathrm{UT}(n,k)$ 为 k 上一切 $n\times n$ 单位上三角矩阵的集合.

性质 5.2.13. *如果 k 是域, 则 $\mathrm{UT}(n,k)$ 是 $\mathrm{GL}(n,k)$ 的子群.*

性质 5.2.14. *设 $q=p^l$, 其中 p 是素数. 对每个 $n\geq 2$,$\mathrm{UT}(n,F_q)$ 是阶为 $q^{\binom{n}{2}}=q^{n(n-1)/2}$ 的 p-群.*

性质 5.2.15. *如果 p 是奇素数, 则存在 p^3 阶非 Abel 群 G 满足对一切 $x\in G$,$x^p=1$.*

证明. 如果 $G=\mathrm{UT}(3,F_p)$, 则 $|G|=p^3$. 现在 G 是非 Abel 群, 例如矩阵:

$$\begin{pmatrix}1&1&0\\0&1&1\\0&0&0\end{pmatrix}\quad\begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix}$$

不交换. 如果 $A\in G$, 则 $A=I+N$, 因 p 是奇素数, $p\geq 3$, 从而 $N^p=0$. 易知形如:

$$a_0 I+a_1 N+\cdots+a_m N^m$$

一切矩阵的集合是一个交换环, 其中 $a_i \in F_p$, 且这个交换环满足对一切 M, $pM = 0$. 由于在每个交换环中二项式定理成立; 因为 $1 < i < p$ 时, 有 $p \mid \binom{p}{i}$, 则有:

$$A^p = (I + N)^p = I^p + N^p = I.$$

□

性质 5.2.16. *令 F_q 表示有 q 个元素的有限域, 则:*

$$| \mathrm{GL}(n, F_q) | = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}).$$

性质 5.2.17. *如果 p 是素数且 $q = p^m$, 则单位上三角矩阵 $\mathrm{UT}(n, F_q)$ 是 $\mathrm{GL}(n, F_q)$ 的 Sylow p-子群.*

5.3 可解群

随着 Galois 理论发展, 引入群可解的概念是自然的, 这里做了进一步的抽象.

定义 5.3.1. 若群 G 有一个下降到 1 的正规列:

$$G = G_0 \triangleright G_1 \triangleright G_2 \dots \triangleright G_n = \{1\}$$

而 G 的因子列:

$$G/G_1, G_1/G_2, \dots, G_{n-1}/G_n$$

若每个商群 G_i/G_{i-1} 都是 Abel 的, 则称 G 是一个**可解群 (solvable)**.

注 59. 形如 $G = G_0 \triangleright G_1 \triangleright G_2$ 的正规关系无法得出形如 $G = G_0 \triangleright G_2$ 的关系.

性质 5.3.2. *(1) 对于一个群 G, 和一个正规子群 H, 若 $H, G/H$ 可解, 则 G 是可解的. (2) 若 G 可解, 那么其子群, 商群, 与另一个可解群的直积也是可解的.*

证明. 略. □

例 5.3.3. $p-$ 群是可解群. 这是因为形如阶为 p^k 的群必然有 p^{k-1} 阶的正规群, 从而其因子列同构于 Abel 群 $\mathbb{Z}_p$.

定义 5.3.4. 对于 $x, y \in G$, 其**交换子 (commutator)** 为:

$$[x, y] = xyx^{-1}y^{-1}$$

注 60. 也就是对于一般不可交换的 x, y, 通过引入交换子使得其交换, 也就是 $xy = [x, y]yx$. 显然, x, y 可以交换当且仅当其交换子为 1. 令人遗憾是的是, 交换子全体无法构成一个群, 其对乘法不封闭, 但可以用它们来生成一个群.

定义 5.3.5. 由全体交换子生成的群称为**交换子群 (commutator subgroup)**. 即为:

$$G' = \langle [x,y] | x,y \in G \rangle$$

注 61. 由于符号上的一撇好似求导, 所以交换子群又有“导群”的别称.

性质 5.3.6. *(1)* $G' \triangleleft G$.

(2) G/G' *是 Abel 的.*

(3) 若有 $H \triangleleft G$, *且* G/H *是 Abel 群, 当且仅当* $G' \subseteq H$.

证明. (1) 对任意的 $a \in G$, 考察:

$$a[x,y]a^{-1} = axyx^{-1}y^{-1}a^{-1} = (axa^{-1})(aya^{-1})(ax^{-1}a^{-1})(ay^{-1}a^{-1}) \in G'$$

(2) 对 $aG', bG' \in G/G'$, 有 $[aG', bG'] = aba^{-1}b^{-1}$.

(3) G/H 是 Abel 的当且仅当, 对于任意的 aH, bH, 有 $[aH, bH] = [a,b]G' = G'$, 其中 G' 是 G/G' 的单位元.

(4) G/H 是 Abel 群当且仅当, 对于任意的 aH, bH, $[aH, bH] = [a,b]H = H$, 当且仅当 $[a,b] \in H$, 当且仅当 $G' \subseteq H$.

□

定义 5.3.7. 群 G 的**导出列 (derived series)** 是指:

$$G = G' \triangleright G^{(2)} \triangleright G^{(3)} \cdots$$

性质 5.3.8. *一个群* G *可解当且仅当, 其导出列下降到* $\{1\}$. *即存在整数* c, *使得* $G^c = \{1\}$.

证明. 导出列是正规列这是显然的. 而反过来可解说明存在正规列:

$$G = G_0 \triangleright G_1 \triangleright G_2 \ldots \triangleright G_n = \{1\}$$

G_0/G_1 是 Abel 群说明 $G^{(1)} \subseteq G_1$. 假设 $G^{(i)} \subseteq G_i$. 因为 G_i/G_{i+1} 是 Abel 的, 所以 $G_i' \subseteq G_{i+1}$. 由此归纳法给出 $G^{(i)} \subseteq G_i$, 那么 $G^{(i+1)} \subseteq (G_i)' \subseteq G_{i+1}$. 由此 $G^{(n+1)} \subseteq G_n = 1$. 于是, 交换子群下降到 $\{1\}$. □

定义 5.3.9. 设 $H \triangleleft G$, 称 H 为 G 的**极小正规子群 (minimal normal subgroup)**, 如果有 $H \neq \{1\}$, 则不存在 $K \triangleleft G$, 使得 $\{1\} \subsetneq K \subsetneq H$.

在证明前先证明个实用结论:

性质 5.3.10. *若有* $H \triangleleft G$, *且* K $\mathrm{Char}\, H$, *则有* $K \triangleleft G$.

证明. 证明是考虑对任意的 $\sigma \in \mathrm{Inn}(H)$, 由于 $H \lhd G$, 所以 $\sigma(H) = H$. 把 σ 限制到 H 上有 $\sigma|_H \in \mathrm{Inn}(H)$. 由于 K Char H, 所以 $\sigma|_H(K) = K$. 即 $K \lhd G$. 特别地, K Char H 可以推出 $K \lhd H$. 反之不对. □

定理 5.3.11. *若 G 是个有限可解群, 则其每个极小子群 H 是初等 Abel 的, 也就是说 H 是 $\mathbb{Z}_p$ 上的线性空间. 事实上, 对于初等 Abel 群, 其每个非平凡的元素有阶 p, 则群的阶必然形如 p^k. 由有限 Abel 群的结构定理可知(4.1.13), 此群同构于有限直和 $\bigoplus \mathbb{Z}_p$.*

证明. 由于 H 是极小正规, $H' \lhd H$, 所以有 $H' = \{1\}$ 或者 $H' = H$. 而 G 可解, 则有子群 H 可解. 故 $H' = \{1\}$, 所以 H 是 Abel 的. 由于 H 是 Abel. 那么 Sylow-p 子群 $P \lhd H$, 且唯一. 同时, 对任意的 $\phi \in \mathrm{Aut}(H)$, 我们有 $|\phi(P)| = |P|$. 故 $\phi(P)$ 也是一个 Sylow-p 子群, 由此 P Char H. 注意到, $H \lhd G$, 则有 $P \lhd G$, 如果 $P \neq H$, 则 $\{1\} \subsetneq P \subsetneq H$ 与 H 的极小性矛盾. 而 $P = H$ 导致 H 是 Abel $p-$ 群. 考虑 p 阶元的群:$B = \{x \in H | x^p = 1\}$. 由于对任意的 $\phi \in \mathrm{Aut}(H)$, 有 $[\phi(x)]^p = \phi(x^p) = \phi(1) = 1$. 于是 B Char H, 以及 $H \lhd G$, 得到 $B \lhd G$, 此时再结合 H 极小正规, 得出 $H = B$. 那么 $x^p = 1$, 对任意的 $x \in H$. 由此 H 可以看作 $\mathbb{F}_p$ 上的线性空间. 由此, 对于可解有限群 G 和其极小正规群 $H \lhd G$, 把 G 共轭作用于 H, 因为 $G(H) = H$, 故此作用合法. 已经证明 H 可看作 $\mathbb{F}_p$ 上的线性空间, 故 G 可以作用于某个 $\mathbb{F}_p$ 上的线性空间. □

引理 5.3.12 (Fraffini Argument 引理). *设 K 为有限群 G 的正规子群, P 为 K 的某个 Sylow$p-$ 子群, 那么 G 可以分解为:*

$$G = KN_G(P)$$

其中 $N_G(P) = \{g \in G | gPg^{-1} = P\}$, P 在 G 中的正规化子.

证明. 对任意的 $g \in G$, $gPg^{-1} \subseteq gKg^{-1} = K$, 由此 gPg^{-1} 构成 K 的另一个 Sylow $p-$ 子群. 故存在 $k \in K$, 使得 $gPg^{-1} = kPk^{-1}$. 这等价于 $k^{-1}gP(k^{-1}g)^{-1} = P$. 由此推出 $k^{-1}g \in N_G(P)$, 由此 $g = k(k^{-1}g) \in KN_G(P)$. □

定理 5.3.13 (P.Hall). *若 G 是有限可解群, $|G| = ab$, $(a, b) = 1$, 那么 G 必然包含有一个阶为 a 的子群.*

证明. 证明是对阶数作归纳. 考虑这个可数集合:

$$\{G | G\text{可解且}|G| = ab, (a, b) = 1\}$$

显然上述集合中最小阶是 $|G| = 1 = 1 \times 1$, 而其自然其有阶为 1 的子群, 也就是其本身. 下面作归纳假设: 在该集合中所有阶比 ab 小的集合都满足定理. 现在我们试图说明, 根据此归纳假设, 可以得出 ab 阶的也是满足定理的. 对于可解群 $|G| = ab$. 另外, 注意到群 G 的任意子群的解都会有类同 $|H| = a'b'$, 其中 $a'|a, b'|b$ 的形式.

(1) 情况一: 假如存在一个正规子群 H, 此时有 $b \nmid |H|$. 那么也就意味着 $b' < b$. 由于 G 可解, 则其商群 $|G/H| = (a/a')(b/b')$ 也可解, 其中 $a/a', b/b'$ 互素. 这说明该商群落在上述集合中, 同时商群的阶小于 $G = ab$, 归纳假设说明商群 $|G/H|$ 满足定理, 也就是存在子群 A/H, 其阶为 a/a', 其中 $H \subseteq A \subseteq G$, A 是 G 的子群, 这是群的第二同构定理保证的. 不难算出 $|A| = |A/H|\,|H| = ab' < ab$, 而 G 的可解导致子群 A 的可解, 由此归纳假设给出 A 的阶为 a 的子群存在, 而这个子群自然也就是 G 的子群. 情况一讨论完毕.

(2) 情况二: 假如其任意的正规子群 H, 有 $b \mid |H|$. 特别的, 取 N 为 G 的极小正规子群. 由于 G 是有限群, 所以这总是存在的. 根据定理(5.3.11), 可知此时 N 为某个初等 Abel 的 p-群. 于是, $b \mid |N|$(此处取 $H = N$) 使我们可以假设 $b = p^m$. 此时 $|G| = ap^m, (a, p^m) = 1$ 导致 N 实际上还是 G 的 Sylow p-群. 此外由于正规的 Sylow 子群是唯一的, 故群 N 是唯一的. 下面我们讨论此特殊情形. 当 G 的阶为 $ap^m, p \nmid a$, 且 G 含有一个正规的交换 Sylow p-子群 H, 且其为 G 唯一的极小正规子群. 首先因为 G 可解, 则 G/H 可解, 于是 $|G/H| = \frac{ap^m}{p^m} = a$. 取 $|G/H|$ 的极小正规子群 $S/H \triangleleft G/H$, 另外由群第三同构定理, 也可以得到 $S \triangleleft G$, 故 S/H 是某个 p-群. 这里的 p 泛指某个素数, 和前文 G 中的阶中的 p 不是一样. 设 $|S/H| = q^m, q$ 是某个素数, 那么 $|S| = |S/H|\,|H| = p^m q^n$, 其中 $S \triangleleft G$. 再取 S 的 Sylow-q 子群 $Q, |Q| = q^n$, 由于集合 HQ 的基数.

$$|HQ| = \frac{|H||Q|}{|H \cap Q|} = \frac{|H||Q|}{|\{1\}|} = p^m q^n = |S|$$

那么有 $S = HQ$. 另外注意到 $H \triangleleft S$, 是 S 的唯一 Sylow -p 子群. 由 $S \triangleleft G$ 和 Q 是 S 的 Sylow 子群, 则根据 Frattini Argument 引理(5.3.12), $G = SN_G(Q)$, 故:

$$G/S = SN_G(Q)/S \cong N_G(Q)/N_G(Q) \cap S = N_G(Q)/N_S(Q)$$

下面说明 $N_G(Q)$ 为要找的群, 即 $|N_G(Q)| = a$. 计算表明:

$$|N_G(Q)| = \frac{|G||N_S(Q)|}{|S|}$$

由于 $S = HQ$, 且 $Q \subset N_S(Q) \subset S$, 则有 $S = HN_S(Q)$. 由此,

$$|S| = |HN_S(Q)| \tag{5.1}$$

$$= \frac{|H||N_S(Q)|}{|H \cap N_S(Q)|} \tag{5.2}$$

回代再次计算 $N_G(Q)$ 的阶可得到:

$$|N_G(Q)| = \frac{|G||N_S(Q)||H \cap N_S(Q)|}{|H||N_S(Q)|} = a|H \cap N|$$

其中, 我们记 $N = N_S(Q)$ 如果 $H \cap N = \{1\}$, 则定理得证. 否则可以进一步说明.

i) $H \cap N \subseteq Z(S)$. 任意取 $x \in H \cap N, s \in S$, 由于 $S = HQ$, 则有 $s = hy$, 其中 $h \in H, y \in Q$. 由于 H 是 Abel 群, 则 x, h 可以交换, 由此问题转化为 x, y 是否可以交换的问题. 由于 $x \in N \subset N_S(Q)$, 那么有 $xyx^{-1} \in Q, y^{-1} \in Q$, 则 $xyx^{-1}y^{-1} \in Q$. 考虑到 $H \triangleleft S$, 以及 H 是唯一 Sylow $p-$ 子群的事实, 我们有 $yx^{-1}y^{-1} \in H, x \in H$. 由此 $xyx^{-1}y^{-1} \in H$. 即 $[x, y] = xyx^{-1}y^{-1} \in H \cap Q = \{1\}$, 这意味着 x, y 可以交换. 故 $H \cap N \subseteq \mathrm{Z}(S)$.

ii) $\mathrm{Z}(S) = \{1\}$. 考虑到 $\mathrm{Z}(S)$ $\mathrm{Char}\, S$, 以及 $S \triangleleft G$, 所以 $\mathrm{Z}(S) \triangleleft G$. 若 $\mathrm{Z}(G) \neq \{1\}$, 那么其包含一个极小正规子群, 而这个群一定是 G 的极小正规子群. 由此, $H \subset \mathrm{Z}(S)$, 因为 H 是 G 的唯一极小正规子群. 但是由于 $S = HQ$, 那么容易看出 Q $\mathrm{Char}\, S$. 由此 $Q \triangleleft G$, 那么有 $H \subset Q$, 矛盾. 由此 $\mathrm{Z}(S) = \{1\}$, $H \cap N = \{1\}$.

由此, $|N_G(Q)| = a$. 情况二得证.

定理得证. □

第六章　有限群的常表示论

6.1　半单环、半单模及半单代数 (二)

Artin—Wedderburn 定理阐述的是与半单环有关的深刻结构定理, 为此我们需要进一步讨论半单环. Artin 将 Wedderburn 结果推广到了一般非交换, 满足链条件 DCC 的半单环 k 上, 为此我们还需要深入讨论满足 DCC 的环, Artin 环. 本节将阐述一些基本概念, 例子和结果.

首先, 我们回顾 DCC 有限性条件(1.2.11), 并给出如下定义:

定义 6.1.1. R 是一个环, L 为 R 的左理想, 称 L 为 R 的一个**极小左理想 (minimal left ideal)**, 如果 $L \neq (0)$, 且不存在左理想 J, 使得 $0 \subsetneqq J \subsetneqq L$.

注意, 并非每一个环 R 都包含极小左理想, 譬如 $\mathbb{Z}$. 但对于一般的环 R, 一定存在极大理想; 对于交换环而言, 每个交换环都包含极小素理想. 自然的问题是, 什么样的环一定含有极小理想? DCC 链条件告诉我们, Artin 环一定存在极小理想.

定理 6.1.2 (极小理想作为 $R-$ 模是单模). *R 是一个环, L 是 R 的极小左理想, 则:*
(1) 每一个极小左理想 L 都是左 $R-$ 单模.
(2) 如果 R 是左 Artin 环, 则每一个非零左理想 I 都包含一个极小左理想.

证明. (1) 如果 S 为 ${}_RL$ 的非零子模, 则由正则模的子模与理想一一对应知, S 也是 R 的包含于 L 的左理想. 由 L 的极小性, $S = L$, 即 ${}_RL$ 没有非平凡子模, 从而 ${}_RL$ 是单模.

(2) 令 $F = \{L \mid \{0\} \subsetneqq S \subseteqq I\}$, $F \neq \varnothing$. 因为 $I \in F$, 由 Artin 条件(1.2.13), F 中存在极小元 L, L 为极小左理想.

□

记号: k 为一个除环, $R = \mathrm{Mat}_n(k)$, 对于任意的 $1 \leq l \leq n$, 记除第 l 列元素全为 0 的矩阵为:

$$\mathrm{COL}(l) = \{[a_{ij}] \in \mathrm{Mat}_n(k) \mid a_{ij} = 0, j \neq l\}$$

记 $k_* = k^{op}$, 如果 $e_1, e_2, \cdots, e_n$ 为左向量空间 k_*^n 的一组基, 根据推论(6.3.5), 有 $R = \mathrm{Mat}_n(k) \cong \mathrm{End}_{k_*}(k_*^n)$, 且:

$$\mathrm{COL}(l) \cong \{T : k_*^n \mapsto k_*^n \mid T(e_j) = 0, j \neq l\}$$

性质 6.1.3. *k 为一个除环, $1 \leq l \leq n$, 则 $\mathrm{COL}(l)$ 为 $\mathrm{Mat}_n(k)$ 的极小左理想.*

证明. 容易验证 $\mathrm{COL}(l)$ 是 $\mathrm{Mat}_n(k)$ 的左理想, 下证其为极小左理想. 记 $k_* = k^{op}$, 因为 $\mathrm{Mat}_n(k) \cong \mathrm{End}_{k_*}(k_*^n)$. 我们采用线性变换的语言, 这样可以避免矩阵的计算. 设 $I \subseteq \mathrm{COL}(l)$ 为一个非零左理想. 现证 $I = \mathrm{COL}(l)$, 即证对任意的 $T \in \mathrm{COL}(l)$, $T \in I$. 因为 I 是理想, 只需要找到 $T^{'} \in I; S \in \mathrm{End}_{k_*}(k_*^n)$, 使得 $T = S \circ T^{'} \in I$ 即可. 取 $0 \neq T^{'} \in I \subseteq \mathrm{COL}(l)$, 使得 $T^{'}(e_l) \neq 0$. 记 $T(e_l) = u \neq 0$. 对于任意 $T \in \mathrm{COL}(l)$, 令 $w = T(e_l)$, $w \neq 0$. 对于 $u, w \neq 0$, 因为除环的反环也是除环, 于是 u, w 确定了一个矩阵, 即存在 $0 \neq S \in \mathrm{End}_{k_*}(k_*^n)$, 使得 $S(u) = w$. 注意到,

$$S \circ T^{'}(e_i) = \begin{cases} 0, & i \neq l \\ S(u) = w = T(e_l), & i = l \end{cases}$$

于是, T 与 $S \circ T^{'}$ 在 k_*^n 的同一组基下作用相同, 于是 $T = S \circ T^{'} \in I$. 故 $\mathrm{COL}(l)$ 是 $\mathrm{Mat}_n(k)$ 的极小左理想.

□

下面, 我们回顾一些半单性的概念.

定义 6.1.4. 称一个环 R 为**单环 (simple ring)**, 如果 $R \neq 0$, 且 R 的双边理想仅有 0 和 R 本身.

性质 6.1.5. *k 是一个除环, 除环上的矩阵环 $R = \mathrm{Mat}_n(k)$ 是单环.*

证明. 取矩阵单位 $\{E_{pq} \mid 1 \leq p, q \leq n\}$ 为 $\mathrm{Mat}_n(k)$ 的一组基. 对于任意的 $A = [a_{ij}] \in \mathrm{Mat}_n(k)$, 存在 A 的唯一表示:

$$A = \sum_{i,j} a_{ij} E_{ij}$$

对于矩阵单位的运算, 我们有如下公式:

$$E_{ij} E_{kl} = \delta_{jk} E_{il}; \quad \text{其中, } \delta_{ij} \text{ 是 Kronecker 符号}$$

设 N 为 $\mathrm{Mat}_n(k)$ 中非零双边理想, 设 $0 \neq A = [a_{ij}] \in N$, 不妨设第 i 行, 第 j 列的元

素 $a_{ij} \neq 0$. 因为 N 为双边理想, 则对于任意的 p, q 成立:

$$E_{pi}AE_{jq} = E_{pi}(\sum_{k,l} a_{kl}E_{kl})E_{jq} \tag{6.1}$$

$$= E_{pi}(\sum_{k} a_{kj}E_{kq}) \tag{6.2}$$

$$= \sum_{k} a_{kj}E_{pi}E_{kq} \tag{6.3}$$

$$= a_{ij}E_{pq} \in N \tag{6.4}$$

因为 $0 \neq a_{ij} \in k$, k 是一个除环, 则 $a_{ij}^{-1} \in k$. 从而 $E_{pq} \in N$. 于是 $\mathrm{Mat}_n(k) \subset N$, $N = \mathrm{Mat}_n(k)$. □

定义 6.1.6. 称 R 为一个**左半单环 (left semisimple)**, 如果 R 是一些极小左理想的直和.

注 62. 右半单环也可以类似的进行定义. 事实上, 我们将会知道, 环 R 是左半单的当且仅当是右半单的.

性质 6.1.7. *R 是一个半单环, 则有以下性质:*

(1) R 是有限个极小左理想的直和.

(2) R 作为正则模 ${}_RR$, 则 R 既是满足 DCC 链条件, 也满足 ACC 链条件, 故半单环上的正则模是有限长度模, 一定具有合成序列.

证明. (1) 从事实(1)即可知道.

(2) 设 $R = L_1 \oplus L_2 \cdots \oplus L_n$, 则 ${}_RR$ 具有以下合成序列:

$$R = L_1 \oplus L_2 \cdots \oplus L_n \supsetneqq L_2 \cdots \oplus L_n \supsetneqq \cdots \supsetneqq L_n \supseteq \{0\}$$

因为 L_i 是极小左理想, 则相应的因子模 ${}_RL_i$ 是单模. 于是, R 既满足 ACC, 也满足 DCC. 对于 $R-$ 模 M 而言, M 有合成序列当且仅当, M 满足 ACC 链条件和 DCC 链条件. 于是 R 作为正则模一定有合成序列.

□

下面, 我们总结半单环及半单模的一些重要结论如下, 它们在第三章已经证明.

定理 6.1.8 (半单环的结构性质). *R 是一个环;*

(1) 以下五条等价:

R 上的模是半单模; R 上的模是内射模; R 上的模是投射模; R 是半单环; $R-$ 模正合列都是可裂正合列.

(2) 半单环的商环是半单环.

(3) 半单环的有限直积是半单环. 特别的, 域是半单模 *(*极小左理想为域本身*)*, 从而有限个域的直积是交换半单环; 事实上, 即将证明的 *Artin—Wedderburn* 定理告诉我们, 交换半单环当且仅当是有限个域的直积.

(4) 域上的有限维仿射空间是交换半单环, 域 k 上的线性空间是半单环, 除环 k 上的左向量空间是半单环.

(5) R 是一个主理想整环, $p_1, p_2, \cdots, p_s$ 是 R 中 s 个互不相同的不可约元 *(*素元*)*, $s \in \mathbb{N}$, 令 $n = p_1 p_2 \cdots p_s$, 则 $R/(n)$ 是半单环.

(6) 半单模的子模和商模是半单模.

(7) 半单模上的单模都对应一个极小左理想.

下面, 我们给出一个重要的半单环的例子, 它是 Artin—Wedderburn 定理的充分性证明.

定理 6.1.9 (**Artin—Wedderburn 定理的充分性**)**.** *Artin—Wedderburn* 定理的充分性证明*:*

(1) k 是一个除环, V/k 是除环上的左向量空间. $\dim_k(V) = n$, 则除环上的矩阵环是半单环*:*

$$\mathrm{End}_k(V) \cong \mathrm{Mat}_n(k^{op})$$

(2) $k_1, k_2, \cdots, k_r$ 是 r 个半单环, 则

$$\mathrm{Mat}_{n_1}(k_1) \times \mathrm{Mat}_{n_2}(k_2) \times \cdots \times \mathrm{Mat}_{n_r}(k_r)$$

也是半单环.

证明. (1) 设 $v_1, v_2, \cdots, v_n$ 是 V 的一组基, 根据推论(6.3.5), 有 $\mathrm{End}_k(V) \cong \mathrm{Mat}_n(k^{op})$, 对于任意的 $1 \leq l \leq n$, 我们知道 $\mathrm{COL}(l)$ 是 $\mathrm{Mat}_n(k^{op})$ 的极小左理想. 同时, 根据矩阵运算, 容易证明 $\mathrm{Mat}_n(k^{op})$ 有如下直和分解:

$$\mathrm{Mat}_n(k^{op}) = \mathrm{COL}(1) \oplus \mathrm{COL}(2) \oplus \cdots \oplus \mathrm{COL}(n)$$

从而, $\mathrm{End}_k(V) \cong \mathrm{Mat}_n(k^{op})$ 是半单环.

(2) 根据半单环的性质(6.1.8)立即得到.

□

注 63. 单环不一定是半单环, 例如 V/k 是域 k 上的无穷维线性空间, $R = \mathrm{End}_k(V)$ 是单环, 但不是半单环.

下面给出单环是半单环的充分条件.

性质 6.1.10. *R 是一个单环, 若 R 还是左 Artin 环, 则 R 是半单环.*

证明. R 是左 Artin 环, 则 R 包含一个极小左理想 L. 同时, ${}_RL$ 是单模. 对于任意的 $a \in R$, 构造左 R-模同态:

$$f_a :_R L \longmapsto_R R$$

$$x \longmapsto x.a$$

于是, $\mathrm{Im}(f_a) = La$. 因为 ${}_RL$ 是单模, 则要么 $\mathrm{Ker}(f_a) = \{0\}$, 要么 $\mathrm{Ker}(f_a) = L$. 即要么 $La = \{0\}$, 要么 $La = L$. 考虑 $I = \langle \bigcup\limits_{a\in A} L_a \rangle = \sum\limits_{a\in R} L_a \subseteq R$. I 是一个双边理想, 首先 I 是左理想, 且 $La \in I$. 对任意 $b \in R$, $(La)b = L(ab) \subseteq I$. 因为 R 是一个单环, 故 $I = R$. 现断言, 存在有限个元素 $a_1, a_2, \cdots, a_n \in R$, 使得

$$R = \left\langle \bigcup_{i=1}^{n} La_i \right\rangle = \sum_{i=1}^{n} La_i$$

因为 $1 \in R$, 则根据理想和的定义, 存在 $n \in \mathbb{N}$, 使得 $1 \in La_1 + La_2 + \cdots + La_n$. 对于任意的 $b \in R$,

$$b = 1 \cdot b \in b(La_1 + La_2 + \cdots + La_n) \subseteq La_1 + La_2 + \cdots + La_n \subseteq R$$

于是, $R = La_1 + La_2 + \cdots + La_n$. 选择 $n = \min\{n \in \mathbb{N} \mid R = La_1 + La_2 + \cdots + La_n\}$. 断言: $R = \bigoplus\limits_{i=1}^{n} La_i$. 否则, 存在 $1 \leq i \leq n$, 使得:

$$La_i \cap (\bigoplus_{j\neq i} La_j) \neq \{0\}$$

因为 $La_i \neq \{0\}$ 是单模. 于是,

$$La_i \cap (\bigoplus_{j\neq i} La_j) = La_i$$

也就是说, $La_i \subseteq \bigoplus\limits_{j\neq i} La_j$. 从而, $R = \bigoplus\limits_{j\neq i} La_j$. 这与 n 的选取矛盾, 于是 $R = \bigoplus\limits_{i=1}^{n} La_i$, 每一个 La_i 是极小左理想. 于是 R 是半单环. □

6.2 群代数与群的表示

对于一般的群论, 环论, 域论, 模论, 及非结合代数李代数等经典的代数结构的研究, 一方面, 我们可以从这些代数结构本身出发, 研究它们的子系统, 商系统, 结构模块, 结构不变量, 全局维数, 局部结构等; 另一方面, 我们可以借助表示论的手段, 考虑某个其他的代数系统 (可以是一般的集合, 线性空间, 交换环, 拓扑空间等) 对我们所研究代数系统的一个" 作用", 研究此作用所得到的复合结构, 对复合结构的研究从而反馈到原代数结构的研究.

定义 6.2.1. k 是一个交换环, V/k 是一个 $k-$ 模, G 是一个群. 群 G 的一个 $k-$ **表示 (k-representation)** 是指如下的一个群同态

$$\sigma : G \mapsto \mathrm{Aut}(V)$$

其中, $\mathrm{Aut}(V)$ 是 $k-$ 模 V 自同构群, V 称为**表示模 (representation module)**. 特别的, 当 k 是一个域时, V 称为**表示空间 (representation space)**, 此时 V 的维数 $\dim_k(V)$ 成为**表示 σ 的次数**, 记作 $\deg(\sigma)$.

注 64. 当 k 为一个域时 (通常考虑 $\mathbb{C}$) 是我们最为关心的情况, 此时 V 是复数域 $\mathbb{C}$ 上的有限维线性空间. 特别的, 如果选定一组基, $\mathrm{Aut}(V) = \mathrm{GL}(V) = \mathrm{GL}(n, \mathbb{C})$.

给定了一个表示, 我们往往会得到一个新的代数结构. 例如, 当我们给定一个群作用时, 等价于给定了一个群到集合全变换群的群同态. 这里我们指出, 给定一个 $k-$ 表示就等价于给定了一个 $kG-$ 模. 其中, kG 是群 G 在域 k 上的群代数.

性质 6.2.2 (给定一个 $k-$ 表示 $\Longleftrightarrow$ 给定一个 $kG-$ 模). *k 是一个交换环, V/k 为一个 $k-$ 模, G 是一个群, $\sigma : G \mapsto \mathrm{Aut}(V)$ 为一个 $k-$ 表示, 则 σ 诱导了 V 上的一个 $kG-$ 模:*

$$kG \times V \mapsto V$$

$$(\sum_{g\in G} a_g g, v) \mapsto (\sum_{g\in G} a_g g).v = \sum_{g\in G} a_g \sigma_g(v)$$

记 σ 诱导的 $kG-$ 模 V 为 V^σ. 反过来, 每一个 $kG-$ 模也都决定一个 $k-$ 表示 σ:

$$\sigma : G \mapsto \mathrm{Aut}(V)$$

$$g \mapsto \sigma_g : v \mapsto g.v$$

证明. 验证模的数乘四条以及 $k-$ 表示的定义即可. □

我们指出, **一个群作用诱导了一个群表示**. 设 X 是一个集合, G 是一个群, k 是一个域, G 对集合 X 上有一个群作用 $G \curvearrowright X$, 于是诱导出群同态 $\sigma : G \mapsto S_X$. V/k 是以 X 中的元素为基生成的域 k 上的线性空间, 其中 $\dim_k(V) = |X|$. 注意到, 任给一个置换 $\tau \in S_X$, 我们可以得到一个 V 的线性变换 T, T 作用到基 X 上是通过 τ 进行的一次置换, 即 $T(x_\alpha) := x_{\tau(\alpha)} \in X, x_\alpha \in X, \alpha$是指标集. 于是, 群作用诱导出了如下单态射:

$$\sigma^* : S_X \mapsto \mathrm{GL}(V)$$

$$\tau \mapsto T : x_\alpha \mapsto T(x_\alpha) = x_{\tau(\alpha)}$$

从而, 令 $\varphi = \sigma^* \circ \sigma : G \mapsto \mathrm{GL}(V) = \mathrm{GL}(\langle X \rangle)$, φ 是一个 $k-$ 表示, 同时也得到相应的 $kG-$ 模 V^φ.

特别的, 根据 Cayley 定理, 每一个群 G 都同构于置换群 S_G 的一个子群, 即存在单群同态 $\delta : G \mapsto S_G$. 事实上, Cayley 定理的证明中, 采用了群 G 对自身的平移作用是忠实的. 令集合 $X = G$, V 是 G 为基在域 k 上生成的线性空间, 定义其上乘法后, 即是群代数 kG. 于是, 我们得到一个 $k-$ 表示, 对应的 $kG-$ 模是群代数的正则模 ${}_{kG}kG$. 表示空间是群代数 kG, 称其为**正则表示 (regular representation)**.

$$G \xrightarrow{\delta} S_G \xrightarrow{\delta^*} \mathrm{GL}(kG)$$

$$g \longrightarrow \delta_g \longrightarrow \delta_g^*$$

例 6.2.3. 下面给出一些常见的表示.

(1) G 是一个有限群, V/k 是域 k 上的线性空间. $\sigma : G \mapsto \mathrm{GL}(V)$ 为一个 $k-$ 表示, 对于任意的 $g \in G$, $\sigma(g) = Id_V$. 称 σ 为**平凡 (trivial)**$k-$ **表示**, 相应的 $kG-$ 模 V^σ 称为**平凡 kG-模**. 此时, V^σ 也是一个 G-集, 自然的有群作用 $G \curvearrowright V$: 对于任意的 $g \in G, g.v = v$. 即群作用 $G \curvearrowright V$ 仅有一个轨道, 从而是**传递群作用 (transitive)**. 于是, 传递群作用诱导的 $k-$ 表示是平凡表示. 特别的, 如果 $\dim_k(V) = 1$, 即 $V \cong k$, 称表示 σ 为**主 (principal)k-表示**, 相应的 kG-模 k^σ 称为**主 kG-模**, 记为 $V_0(k)$ 其中 σ 如下:

$$\sigma : G \mapsto k$$

$$g \mapsto 1_k$$

(2) G 是一个群, V/k 是域 k 上的 n 线性空间, $\sigma : G \mapsto \mathrm{GL}(V)$ 是一个 k-表示, 取定 V 的一组基 X, 从而 $\mathrm{GL}(n, k) \cong \mathrm{GL}(V)$, 则 $\sigma : G \mapsto \mathrm{GL}(n, k)$. 称 σ 为 G 关于 V 在基 X 的**矩阵表示 (matrix representation)**.

对于表示, 一个自然的问题是, 两个表示何时等价? 也就是说, 两个表示何时诱导的 kG-模是同构的. 下面的定理回答了此问题.

定理 6.2.4 (表示等价). *G 是一个群, k 是一个交换环, V/k 是交换环 k 上的模.σ, τ 是两个 k-表示:*

$$\sigma : G \mapsto \mathrm{GL}(V)$$

$$\tau : G \mapsto \mathrm{GL}(V)$$

则 σ, τ 诱导的 $kG-$ 模同构 $V^\sigma \cong V^\tau$ 当且仅当, 存在 k-模同构 $\varphi \in \mathrm{Aut}(V)$ 使得 σ 和 τ 缠结 (intertwine), 即对于任意的 $g \in G$, $\varphi \circ \tau(g) = \sigma(g) \circ \varphi$.

证明. $(\Rightarrow)$: 设 $\varphi : V^\sigma \mapsto V^\tau$ 是 kG-模同构. 于是, φ 也是 $k-$ 模同构, 且满足:

$$\varphi((\sum_{g\in G} a_g g).v) = (\sum_{g\in G} a_g g).\varphi(v), \quad \forall v \in, \forall g \in G$$

根据 σ 诱导 $kG-$ 模 V^σ 有: $g.v = \sigma(g)(v)$; 根据 τ 诱导 $kG-$ 模 V^τ 有: $g.v = \tau(g)(v)$; 于是对于任意的 $v \in V$,

$$\varphi(\tau(g)(v)) = \varphi(g.v) = g.\varphi(v) = \sigma(g)(\varphi(v))$$

于是得, 对任意 $g \in G$ 有:

$$\varphi \circ \tau(g) = \sigma(g) \circ \varphi$$

$(\Leftarrow)$: 假设存在 $\varphi \in \mathrm{Aut}(V)$, 对任意的 $g \in G$, 使得 $\varphi \circ \tau(g) = \sigma(g) \circ \varphi$. 于是, 对于任意的 $v \in V$, 有如下等式:

$$g.\varphi(v) = \sigma(g)(\varphi(v)) = \varphi(\tau(g)(v)) = \varphi(g.v)$$

又注意到 φ 是 $k-$ 模同构, 于是自然地保持数乘, 即有

$$\varphi((\sum_{g\in G} a_g g).v) = (\sum_{g\in G} a_g g).\varphi(v)$$

□

上述定理采用矩阵的语言, 则得到矩阵表示的等价刻画. 两个 $k-$ 表示等价, 当且仅当它们是相似的.

定理 6.2.5. *G 是一个群, k 是一个交换环, $\sigma, \tau : G \mapsto \mathrm{GL}(n,k)$, 则 $(k^n)^\sigma \cong (k^n)^\tau$ 当且仅当, 存在 $P \in \mathrm{GL}(n,k)$, 对于任意的 $g \in G$, $P\tau(x)P^{-1} = \sigma(g)$.*

证明. 对于交换环上自由模 k^n(IBN), 选定一组基, 则 $\mathrm{GL}(k^n) \cong \mathrm{GL}(n,k)$, 从而用上述定理即可. □

根据 Maschke 定理(2.3.20), 有限群的表示被分为两部分: 有限群的常表示和有限群的模表示. 下面给出具体的阐述形式.

定义 6.2.6. G 是一个有限群, k 是一个域. 根据 Maschke 定理(2.3.20), 当 $\mathrm{Char}\, k \nmid |G|$, 此时群代数 kG 是半单代数, 相应的 $kG-$ 模是半单模, 其决定的表示称为**有限群的常表示 (ordinary representation)**. 如果 $\mathrm{Char}\, k \mid |G|$, 此时群代数 kG 不是半单代数, 相应的 $kG-$ 模不是半单模, 其决定的表示称为**有限群的模表示 (modular representation)**.

6.3 Artin—Wedderburn 定理

Artin—Wedderburn 定理是表示论当中重要的结构定理, Wedderburn 对半单 $k-$ 代数 (k 是一个域) 证明了存在性和唯一性定理, E.Artin 将 Wedderburn 结果推广到一般非交换, 满足链条件 DCC 的半单环 k 上, 这也是 Artin 环的名称缘由. 当时, 因为技术和工具的缺乏, Artin—Wedderburn 定理的证明较为复杂. 随着同调代数的发展, Rotman 采用了同调代数工具给出了证明. 正是得益于同调代数, 我们可以直接对对象和态射进行运算, 避免了譬如构造同态等大量元素的语言使用, 从而使得证明过程简单明了. 为此, 我们先介绍一些同调代数的工具, 便于证明的展开.

6.3.1 同调代数的准备

我们首先回顾 Hom 函子的保持直和与直积的性质, 并且引入模同态的矩阵表示及运算. R 是一个环, A, B 是左 $R-$ 模, $A = \bigoplus\limits_{i=1}^{n} A_i$, $B = \bigoplus\limits_{j=1}^{m} B_j$, 从而对于 Hom 函子, 我们有:

$$\mathrm{Hom}_R(A,B) \cong \mathrm{Hom}_R(\bigoplus_{i=1}^{n} A_i, \bigoplus_{j=1}^{m} B_j) \cong \bigoplus_{i=1}^{n}\bigoplus_{j=1}^{m} \mathrm{Hom}_R(A_i, B_j)$$

在无限代数扩张的 Galois 理论时, 我们介绍过正向极限和逆向极限. 其中, 正向极限是直和, 余积, 推出, 余核, 集合并的推广; 反向极限是直积, 积, 拉回, 核, 集合交的推广. 下面, 我们列出关于正向极限和逆向极限的重要结论以及一些应用.

定义 6.3.1. $\mathcal{C}$ 和 $\mathcal{D}$ 是两个范畴, (F,G) 是一对函子. 其中 $F : C \mapsto D$, $G : D \mapsto C$. **称** (F,G) **为伴随函子对 (adjoint pair)**, 如果对于任意 $\mathcal{C}$ 中的对象 C, 任意 $\mathcal{D}$ 中的对象 D, 有如下自然同构:

$$\tau_{C,D} : \mathrm{Hom}_D(FC, D) \mapsto \mathrm{Hom}_C(C, GD)$$

即对 C 和 D 分别有自然同构如下:
对于任意的 $C \in \mathrm{obj}\,\mathcal{C}$, 固定 $D \in \mathrm{obj}\,\mathcal{D}$, 态射 $f : C \mapsto C'$, 有如下交换图:

$$\begin{array}{ccc} \mathrm{Hom}_D(FC, D) & \xrightarrow{(Ff)_*} & \mathrm{Hom}_D(FC', D) \\ \downarrow{\scriptstyle \tau_{C,D}} & & \downarrow{\scriptstyle \tau_{C',D}} \\ \mathrm{Hom}_C(C, GD) & \xrightarrow{f_*} & \mathrm{Hom}_C(C', GD) \end{array}$$

对于任意的 $D \in \mathrm{obj}\,\mathcal{D}$, 固定 $C \in \mathrm{obj}\,\mathcal{C}$, 态射 $g : D \mapsto D'$, 有如下交换图:

$$\begin{array}{ccc} \mathrm{Hom}_D(FC, D) & \xrightarrow{g^*} & \mathrm{Hom}_D(FC, D') \\ \downarrow{\scriptstyle \tau_{C,D}} & & \downarrow{\scriptstyle \tau_{C,D'}} \\ \mathrm{Hom}_C(C, GD) & \xrightarrow{(Gg)^*} & \mathrm{Hom}_C(C, GD') \end{array}$$

其中, 称 F 为**左伴随 (left adjoint)**, G 为**右伴随 (right adjoint)**.

定理 6.3.2 (极限的性质). *I 为偏序集, $\mathcal{C}$ 为范畴, I 在范畴 $\mathcal{C}$ 上的正向系统为*

$$\{M_i; \psi_i^j\}_{i \in I}$$

I 在范畴 $\mathcal{C}$ 上的反向系统为

$$\{N_i; \varphi_i^j\}_{i \in I}$$

A, B 是范畴 $\mathcal{C}$ 中的对象, 则以下性质成立.

(1) 反变右 Hom 函子把正向极限变成反向极限:

$$\mathrm{Hom}_C(\varinjlim M_i, B) \cong \varprojlim \mathrm{Hom}_C(M_i, B)$$

(2) 共变左 Hom 函子保持反向极限: $\mathrm{Hom}_C(A, \varprojlim N_i) \cong \varprojlim \mathrm{Hom}_C(A, N_i)$.

(3) 张量函子保持正向极限: $\mathcal{C}$ 为模范畴时, $A \otimes \varinjlim M_i = \varinjlim (A \otimes M_i)$.

(4) 偏序集 I 是定向集, 指对于任意的 $i \in I, j \in J$, 存在 $k \in I$, 使得 $i \prec k, j \prec k$. 定向集上的正向系统的正向极限保持正合列: 设定向集 I 在范畴 $\mathcal{C}$ 上的正向系统为 $\{A_i; \alpha_i^j\}_{i \in I}$, $\{B_i; \beta_i^j\}_{i \in I}$, $\{C_i; \gamma_i^j\}_{i \in I}$, 如果存在如下正合列:

$$0 \longrightarrow A_i \xrightarrow{r_i} B_i \xrightarrow{s_i} C_i \longrightarrow 0$$

则正向极限保持正合有:

$$0 \longrightarrow \varinjlim A_i \xrightarrow{r^*} \varinjlim B_i \xrightarrow{s^*} \varinjlim C_i \longrightarrow 0$$

(5) **伴随同构定理** ***(Adjoint Isomorphism):*** *R, S 是环, A 是右 R-模, B 是 (R, S)-双模, C 是左 $S-$ 模, 则存在伴随对:*

$$(\_ \otimes_R B, \mathrm{Hom}_S(B, \_))$$

存在如下函子的伴随同构:

$$\mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \cong \mathrm{Hom}_S(A \otimes_R B, C)$$

(6) (F,G) 是范畴 $\mathcal{C},\mathcal{D}$ 的伴随对, 左伴随 F 保持正向极限, 右伴随保持反向极限.

(7) 特别的, 直和是正向极限, 直积是反向极限, 于是有以下结果:

$$\mathrm{Hom}_C(\bigoplus_{i\in I} M_i, B) \cong \prod_{i\in I} \mathrm{Hom}_C(M_i, B)$$

$$\mathrm{Hom}_C(A, \prod_{i\in I} N_i) \cong \prod_{i\in I} \mathrm{Hom}_C(A, N_i)$$

当 $\mathcal{C}$ 为模范畴时,

$$A \otimes \bigoplus_{i\in I} M_i = \bigoplus_{i\in I} (A \otimes M_i)$$

证明. 参考 Joseph.Rotman 的《An Introduction to Homological Algebra》,Page 243—268. □

R 是一个环, A,B 是左 $R-$ 模, $A = \bigoplus\limits_{i=1}^{n} A_i$, $B = \bigoplus\limits_{j=1}^{m} B_j$, 从而对于 Hom 函子, 我们有:

$$\mathrm{Hom}_R(A,B) \cong \mathrm{Hom}_R(\bigoplus_{i=1}^{n} A_i, \bigoplus_{j=1}^{m} B_j) \cong \bigoplus_{i=1}^{n}\bigoplus_{j=1}^{m} \mathrm{Hom}_R(A_i, B_j)$$

我们引入模同态的矩阵表示, 则有:

$$\bigoplus_{i=1}^{n}\bigoplus_{j=1}^{m} \mathrm{Hom}_R(A_i,B_j) := \begin{bmatrix} \mathrm{Hom}_R(A_1,B_1) & \cdots & \mathrm{Hom}_R(A_n,B_1) \\ \vdots & \vdots & \vdots \\ \mathrm{Hom}_R(A_1,B_m) & \dots & \mathrm{Hom}_R(A_n,B_m) \end{bmatrix}$$

设 $\alpha_i : A_i \mapsto A$, $p_j : B \mapsto B_j$, 对于任意的 $f \in \mathrm{Hom}_R(A,B)$, (α_i, p_j, f) 唯一确定了:

$$f_{ji} = p_j \circ f \circ \alpha_i : A_i \mapsto B_j$$

于是, f 确定了一个广义的 $m \times n$ 阶矩阵 $[f_{ji}]_{m\times n}$:

$$\Phi : \mathrm{Hom}_R(A,B) \longmapsto \bigoplus_{i,j} \mathrm{Hom}_R(A_i,B_j)$$

$$f \longmapsto [f_{ji}]$$

这里称为广义矩阵的原因在于, 矩阵中的不同位置的元素并不属于同一个代数系统. 如果 C 也是左 $R-$ 模, 且 $C = \bigoplus\limits_{k=1}^{l} C_k$, $g \in \mathrm{Hom}_R(B,C)$, $\beta_j : B_j \mapsto B$, $q_k : C \mapsto C_k$ 则 (β_j, q_k, g) 唯一决定了:

$$g_{kj} = q_k \circ g \circ \beta_j : B_j \longmapsto C_k$$

于是, g 确定了一个广义的 $l\times n$ 阶矩阵 $[g_{kj}]_{l\times n}$:

$$\Psi:\mathrm{Hom}_R(B,C)\longmapsto\bigoplus_{j,k}\mathrm{Hom}_R(B_j,C_k)$$

$$g\longmapsto[g_{kj}]$$

现在, $g\circ f\in\mathrm{Hom}_R(A,C)$. $g\circ f$ 决定了一个广义的 $l\times m$ 阶矩阵:

$$\Delta:\mathrm{Hom}_R(A,C)\longmapsto\bigoplus_{i,k}\mathrm{Hom}_R(A_i,C_k)$$

$$g\circ f\longmapsto[(g\circ f)_{ki}]$$

其中,

$$\sum_j g_{kj}\circ f_{ji}=\sum_j q_k g\beta_j\circ p_j f\alpha_i=q_k g(\sum_j\beta_j\circ p_j)f\alpha_i=q_k gf\alpha_i=(g\circ f)_{ki}$$

下面, 我们把上述模同态的广义矩阵表示在模自同态下变成真正的矩阵.

性质 6.3.3. *R 是一个环, $V=\bigoplus_{i=1}^n V_i$ 为一个左 $R-$ 模. L 是一个左 $R-$ 模, 且对于任意的 i, 存在模同构 $V_i\cong L$, 则成立如下环同构:*

$$\mathrm{End}_R(V)\cong\mathrm{Mat}_n(\mathrm{End}_R(L))$$

证明.

$$\mathrm{End}_R(V)=\mathrm{Hom}_R(V,V)=\mathrm{Hom}_R(\bigoplus_{i=1}^n V_i,\bigoplus_{i=1}^n V_i)=\bigoplus_{i,j}\mathrm{Hom}_R(V_i,V_j)$$

因为对任意的 i, $V_i\cong L$, 则 $\mathrm{Hom}_R(V_i,V_j)=\mathrm{End}_R(L)$, 于是有:

$$\mathrm{End}_R(V)=\bigoplus_{i,j}\mathrm{Hom}_R(V_i,V_j)\cong\bigoplus_{i,j}\mathrm{End}_R(L,L)=\mathrm{Mat}_n(\mathrm{End}_R(L))$$

□

性质 6.3.4. *R 是一个环, M 为一个左 $R-$ 模. $M=B_1\oplus B_2\oplus\cdots\oplus B_r$, 且对任意的 $i\neq j$, $\mathrm{Hom}_R(B_i,B_j)=\{0\}$, 则存在环同构:*

$$\mathrm{End}_R(M)\cong\mathrm{End}_R(B_1)\times\cdots\times\mathrm{End}_R(B_r)$$

证明. 根据 Hom 函子的性质,

$$\mathrm{End}_R(M)=\mathrm{Hom}_R(M,M)\cong\prod_{i=1}^r\mathrm{Hom}_R(B_i,\bigoplus_{j=1}^r B_j)$$

因为模范畴是 Abel 范畴, 有限直和与有限直积同构, 于是

$$\bigoplus_{j=1}^{r} B_j \cong \prod_{j=1}^{r} B_j$$

所以,

$$\mathrm{End}_R(M) \cong \prod_{i=1}^{r} \mathrm{Hom}_R(B_i, \bigoplus_{j=1}^{r} B_j) \cong \prod_{i=1}^{r} \mathrm{Hom}_R(B_i, \prod_{j=1}^{r} B_j)$$

而对任意的 $i \neq j$, $\mathrm{Hom}_R(B_i, B_j) = \{0\}$, 则:

$$\mathrm{End}_R(M) \cong \prod_{i=1}^{r} \prod_{j=1}^{r} \mathrm{Hom}_R(B_i, B_j) \cong \mathrm{End}_R(B_1) \times \cdots \times \mathrm{End}_R(B_r)$$

□

事实 2. 注意到对于一般的交换环 R 及其反环 R^{op}, 我们有如下两个基本的事实:

(1) $\mathrm{Mat}_n(R^{op}) \cong (\mathrm{Mat}_n(R))^{op}$.

(2) R 作为正则模的模同态环满足: $\mathrm{End}_R(R) \cong R^{op}$.

(3) 除环 Δ 的反环 Δ^{op} 仍为除环, 且一般 $\Delta \ncong \Delta^{op}$. 但四元数环 $\mathbb{H}$ 作为除环满足: $\mathbb{H} \cong \mathbb{H}^{op}$.

推论 6.3.5. *k 是一个除环, V/k 是 n-维左向量空间, 则:*

$$\mathrm{End}_k(V) \cong (\mathrm{Mat}_n(k))^{op}$$

证明. 因为 $\dim_k(V) = n$, 于是 $V \cong \bigoplus_{i=1}^{n} V_i$, 其中 $\dim_k V_i = 1$, $V_i \cong k$. 于是, 根据性质(6.3.3), 我们有如下同构:

$$\mathrm{End}_k(V) \cong \mathrm{Mat}_n(\mathrm{End}_k(k)) \cong \mathrm{Mat}_n(k^{op}) \cong (\mathrm{Mat}_n(k))^{op}$$

□

6.3.2 存在性定理 (结构)

下面, 我们给出 Schur 引理, 它在各种表示论当中都有不同的版本, 但都起着极为重要的作用, 原因在于他刻画了完全可约模之间的关系.

定理 6.3.6 (Schur 引理). *R 是一个环, M, M' 是左 R-单模. 则成立:*

(1) 如果 $f : M \longmapsto M'$ 为非零 R-模同态, 则 f 为同构.

(2) $\mathrm{End}_R(M)$ *是除环.*

证明. (1) $f : M \longmapsto M^{'}$ 为非零 R-模同态, 则 $\mathrm{Im}(f) \neq \{0\}$; $\mathrm{Ker}(f) \neq M$. 又因为 $\mathrm{Im}(f) \leq M^{'}$, $\mathrm{Ker}(f) \leq M$, 且 $M, M^{'}$ 均为单模. 于是 $\mathrm{Ker}(f) = \{0\}; \mathrm{Im}(f) = M^{'}$. 由模同态第一同态定理:

$$M = M/\mathrm{Ker}(f) \cong \mathrm{Im}(f) = M^{'}$$

(2) $f : M \longmapsto M$ 为 f 的一个非零 R-模同态, 则 f 为同构. 于是 $f^{-1} \in \mathrm{End}_R(k)$ 也是同构. 即 $\mathrm{End}_R(k)$ 是除环.

□

注 65. 总结 Schur 引理的信息, 我们有:

(1) 单模的自同态环为除环.

(2) 单模间的非零模同态必为同构.

(3) L 为环 R 的极小左理想, 则 $R-$ 模同态环 $\mathrm{End}_R(M)$ 是除环.

下面是一个 Schur 引理关于极小左理想的推论, 它贯彻本节几乎所有证明.

引理 6.3.7. *R 为一个环, $L, L^{'}$ 为环 R 的极小左理想. 则下述命题具有递推关系, 其中 (2) 与 (3) 等价. 特别地, 如果 $L^2 \neq (0)$, 则下述三个命题等价.*

(1) $LL^{'} \neq (0)$.

(2) $\mathrm{Hom}_R(L, L^{'}) \neq \{0\}$, *且存在* $b^{'} \in L^{'}$, $L^{'} = Lb^{'}$.

(3) ${}_RL \cong_R L^{'}$.

证明. (1) $LL^{'} \neq (0)$. 则存在 $b \in L$, $b^{'} \in L^{'}$. $bb^{'} \neq 0$. 构造非零 R-模同态, 此处选取右平移:

$$f : L \longmapsto L^{'}$$

$$x \longmapsto xb^{'}$$

于是, $\mathrm{Hom}_R(L, L^{'}) \neq \{0\}$. 同时, 因为 $\mathrm{Im}(f) = Lb^{'} \leq L^{'}$, 而 ${}_RL^{'}$ 为单模, 故 $L^{'} = Lb^{'}$.

(2) $\mathrm{Hom}_R(L, L^{'}) \neq \{0\}$, 则存在 $0 \neq f : L \longmapsto L^{'}$. 注意到 ${}_RL, {}_RL^{'}$ 是单模, 由 Schur 引理, f 为同构. 于是 ${}_RL \cong_R L^{'}$.

(3) 如果 $L^2 =\neq \{0\}$, 则存在 $x, y \in L$, $xy \neq 0$. 因为 ${}_RL \cong_R L^{'}$, 设 g 为 R-模同构, 则

$$0 \neq g(xy) = xg(y) \in LL^{'}$$

于是 $LL^{'} \neq (0)$.

□

我们已经知道, 环 R 的极小左理想作为 R-模是单模. 下面, 我们指出当 R 是半单环时, 每一个 R-单模都同构于环 R 的一个极小左理想. 我们将采取两种不同的证明方法, 一种是采用同调代数的工具, 一种是合成序列的工具. 读者可仔细比较, 体会同调代数的好处.

定理 6.3.8 (半单环上的单模都同构于某个极小左理想). *$R = L_1 \oplus L_2 \oplus \cdots \oplus L_n$ 为左半单环. L_p 为极小左理想. 每一个左 R-单模都同构于某个 L_p.*

证明. (1) 方法一:

设 S 为非零 R-单模. 根据 Hom 函子自然同构于模范畴到 Abel 范畴的恒等函子. 我们有:

$$\{0\} \neq S \cong \mathrm{Hom}_R(R, S) \cong \mathrm{Hom}_R(\bigoplus_{i=1}^{n} L_i, S)$$

由定理(6.3.2), 反变右 Hom 函子把正向极限变成反向极限:

$$\mathrm{Hom}_R(\bigoplus_{i=1}^{n} L_i, S) \cong \prod_{i=1}^{n} \mathrm{Hom}_R(L_i, S) \neq \{0\}$$

于是存在 p, $\mathrm{Hom}_R(L_p, S) \neq \{0\}$. 而 S 和 L_p 都是左 R-单模, 由引理(6.3.7)可知

$$_RS \cong_R L$$

(2) 方法二: S 是单模, 根据单模的等价刻画定理(2.3.5)知, 存在 R 的极大理想 I, 使得 $S \cong R/I$. 于是, 我们有 R-模序列如下:

$$R \supseteq I \supseteq \{0\}$$

因为 R 是半单环, 从而 R 有合成序列如下:

$$R = L_1 \oplus L_2 \cdots \oplus L_n \supsetneqq L_2 \cdots \oplus L_n \supsetneqq \cdots \supsetneqq L_n \supseteq \{0\}$$

根据 Schreier 加细定理(1.4.3)知, 两个序列有着等价的加细. 于是, 存在 $L_p \cong S$.

例 6.3.9. *G 为一个群, k 为一个域. 因为 $\dim_k V_0(k) = 1$, 所以 $V_0(k)$ 是为平凡 kG-模. 根据定理(6.3.8), 存在 kG 唯一一个极小左理想 L, 使得 $_{kG}L \cong V_0(k)$. 下面, 我们寻找*

这个极小左理想 L.

$$\begin{aligned} V_0(k) \cong_{kG} L &= \{u \in kG \mid h.u = u; \forall h \in kG\} \\ &= \{u = \sum_{g\in G} a_g g \in kG \mid h.u = h.(\sum_{g\in G} a_g g) = u; \forall h \in kG\} \\ &= \{u = \sum_{g\in G} a_g g \mid \sum_{g\in G} a_g hg = u = \sum_{g\in G} a_g g\} \\ &= \{u = \sum_{g\in G} a_g g \mid \sum_{g\in G} a_{gh} g = \sum_{g\in G} a_g g = u\}(\text{这是因为求和 g 的任意性}) \end{aligned} \tag{6.5}$$

于是, 对于任意的 $g, h \in G$, $a_g = a_{hg}$. 特别地, 对于任意的 $h \in G$, $a_1 = a_h$. 于是, 对于任意的 $g \in G$, $a_g = a_1$; 即 ${}_{kG}L$ 中的各项系数 a_g 相等. 于是, 令

$$\gamma = \sum_{g\in G} g$$

$$V_0(k) \cong_{kG} L = \{u \in kG \mid u = c\gamma; c \in k\} =_k \langle\gamma\rangle$$

即 $V_0(k) \cong L$ 是域 k 上 γ 生成的一维线性空间. 特别地, 根据 L 的寻找以及生成元知, L 是唯一的.

□

下面, 我们对半单环 R 上同构的单模 (极小左理想) 以直和的形式进行归类, 可类比于多项式的合并同类项, 以归类后的项作为半单环的结构块.

定义 6.3.10. R 是一个左半单环, 则 $R = L_1 \oplus L_2 \cdots \oplus L_n$. 其中 $L_p (1 \le p \le n)$ 是极小左理想. 对极小左理想进行排序, 使得前 r 个极小左理想互不同构; 对于 $m \ge r$, 存在 $1 \le p \le r$, 使得 $L_m \cong L_p$. 记所有与 $L_i (1 \le i \le r)$ 同构的极小左理想的直和为:

$$B_i = \bigoplus_{L_p \cong L_i} L_p$$

称 B_i 为 R 关于分解 $R = \bigoplus_{i=1}^{n} L_i$ 的**单直和因子 (simple components)**.

注 66. 半单环的单直和因子不依赖于具体分解形式.

经过充分的准备, 下面我们给出 Artin—Wedderburn 定理的存在性证明.

定理 6.3.11 (Artin—Wedderburn 定理 I). *R 是一个左半单环, 当且仅当 R 同构于有限个除环上的矩阵环的直积; 即存在除环 $k_1, k_2, \cdots, k_r$,*

$$R \cong \mathrm{Mat}_n(k_1) \times \mathrm{Mat}_n(k_2) \times \cdots \times \mathrm{Mat}_n(k_r)$$

证明. 充分性: 已经证明. 参见定理(6.1.9).
必要性: R 是一个半单环, 则 R 是有限个极小左理想的直和:

$$R = L_1 \oplus L_2 \cdots \oplus L_n$$

进一步, R 可以写成单直和因子的直和:

$$R = B_1 \oplus B_2 \cdots \oplus B_r$$

其中, $B_i = \bigoplus\limits_{L_p \cong L_i} L_p$. 注意到, 对于任意的 $i \neq j$ 有, 由引理(6.3.7):

$$\mathrm{Hom}_R(B_i, B_j) = \mathrm{Hom}_R\left(\bigoplus_{L_p \cong L_i} L_p, \bigoplus_{L_{p'} \cong L_j} L_{p'}\right) = \bigoplus_{L_p \cong L_i; L_{p'} \cong L_j} \mathrm{Hom}_R(L_p, L_{p'}) = \{0\}$$

根据事实(2)知, $R^{op} \cong \mathrm{End}_R(R)$. 而对于任意的 $i \neq j$, $\mathrm{Hom}_R(B_i, B_j) = \{0\}$. 从而根据性质(6.3.4)我们有:

$$R^{op} \cong \mathrm{End}_R(R) = \mathrm{End}_R(B_1 \oplus B_2 \cdots \oplus B_r) = \mathrm{End}_R(B_1 \times B_2 \cdots \times B_r)$$

由因为 $\mathrm{End}_R(B_i) = \mathrm{End}_R(\bigoplus\limits_{L_p \cong L_i} L_p)$, 根据性质(6.3.3)得:

$$R^{op} = \prod_{i=1}^{r} \mathrm{End}_R(\bigoplus_{L_p \cong L_i} L_p) \cong \prod_{i=1}^{n} \mathrm{Mat}_{n_i}(\mathrm{End}_R(L_i))$$

于是,

$$R \cong \left(\prod_{i=1}^{n} \mathrm{Mat}_{n_i}(\mathrm{End}_R(L_i))\right)^{op}$$

因为 L_i 是极小左理想, 则 ${}_RL_i$ 是左 R-单模. 根据 Schur 引理(6.3.6)知, $\mathrm{End}_R(L_i)$ 是除环, 记为 Δ_i. 于是,

$$R \cong \left(\prod_{i=1}^{n} \mathrm{Mat}_{n_i}(\Delta_i)\right)^{op} \cong \prod_{i=1}^{n} \mathrm{Mat}_{n_i}(\Delta_i)^{op}$$

根据事实(2), 除环的反环仍为除环. 于是 Δ_i^{op} 也是反环, 记为 k_i. 从而, 存在有限个除环 $k_1, k_2, \cdots, k_r$, 使得:

$$R \cong \mathrm{Mat}_n(k_1) \times \mathrm{Mat}_n(k_2) \times \cdots \times \mathrm{Mat}_n(k_r)$$

□

注 67. Artin—Wedderburn 定理揭示了半单环的结构, 正如我们所想, 半单环的结构块是一些单环 (除环上的矩阵环是单环, 参考性质(6.1.5)). 这些单环比较特殊, 它们是除环上的矩阵环. 下面的推论告诉我们, 除环和矩阵环都是典型的非交换环, 而以它们为基本结构搭建的半单环并不依赖于交换性. 正是不依赖于交换性, 半单环有着非常好的性质. 特别的, 当半单环是交换环时, 它退化为有限个域的直积.

下面, 我们给出 Artin—Wedderburn 定理一些推论.

推论 6.3.12. *环 R 是左半单环, 当且仅当 R 是右半单环.*

证明. R 是右半单环, 当且仅当 R^{op} 是左半单环. 根据 Artin—Wedderburn 定理(6.3.11) 存在有限个除环

$$k_1, k_2, \cdots, k_r$$

使得:

$$R^{op} \cong \mathrm{Mat}_n(k_1) \times \mathrm{Mat}_n(k_2) \times \cdots \times \mathrm{Mat}_n(k_r)$$

根据反环的性质, 上述同构当且仅当:

$$R \cong \left(\prod_{i=1}^{n} \mathrm{Mat}_{n_i}(k_i)\right)^{op} \cong \prod_{i=1}^{n} \mathrm{Mat}_{n_i}(k_i)^{op}$$

除环 k^i 的反环 k_i 也是除环, 于是 R 是左半单环. □

推论 6.3.13. *R 是一个交换环, 则 R 是半单环当且仅当, R 同构于有限个域的直积.*

证明. R 半单, 根据 Artin—Wedderburn 定理(6.3.11)知, 存在有限个除环 $k_1, k_2, \cdots, k_r$; 使得

$$R^{op} \cong \mathrm{Mat}_n(k_1) \times \mathrm{Mat}_n(k_2) \times \cdots \times \mathrm{Mat}_n(k_r)$$

因为 R 交换, 则对于任意的 i, $\mathrm{Mat}_{n_i}(k_i)$ 交换. 这当且仅当对于任意的 i, $n_i = 1$, k_i 为域. 这等价于

$$R \cong \prod_{i=1}^{r} k_i$$

对于任意的 i, k_i 为域. □

推论 6.3.14. *A 是一个左 Artin 环, 且 A 为单环, 则存在唯一的除环 k, 使得 $A \cong \mathrm{Mat}_n(k)$. 特别地, 除环 k 满足 $k^{op} \cong \mathrm{End}_A(L)$, 其中 L 为 Artin 单环中在同构意义下唯一的极小左理想.*

证明. 我们给出两种方法, 一种是采用同调代数的语言证明存在性; 一种采用传统构造同构的语言证明唯一性. 这有助于更好理解表示论的思想和同调代数工具的好处.

(A) 存在性 (Artin—Wedderburn 定理的推论): 根据性质(6.1.10)的证明过程, 在同构的意义下, A 仅有一类极小左理想, 记为 L. 从而 A 的单直和因子仅有一个, 记为 B. 于是,

$$A \cong (\mathrm{End}_A(A))^{op} = (\mathrm{End}_A(B))^{op} \cong (\mathrm{Mat}_n(\mathrm{End}_A(L)))^{op} \cong \mathrm{Mat}_n(\mathrm{End}_A(L)^{op})$$

根据 Schur 引理(6.3.6)知 $\mathrm{End}_A(L)$ 是除环; 根据事实(2)知除环的反环是除环, 故记 $k = (\mathrm{End}_A(L))^{op}$ 是除环. 从而,

$$A \cong \mathrm{Mat}_n(k)$$

(B) 唯一性 (借助表示论的思想): 假设存在除环 k, 使得 $\mathrm{Mat}_n(k) \cong A$, 则 $k^{op} \cong \mathrm{End}_A(L)$. 用表示论的观点, 不妨令 $A = \mathrm{Mat}_n(k)$, $L = \mathrm{COL}(1)$. 令

$$\varphi : k \longmapsto \mathrm{End}_A(L)$$

$$d \longmapsto \varphi_d : l \mapsto ld$$

现证明 ϕ 为反同构.

(1) 对于任意的 $d \in k$, ϕ_d 是良定义的. 即 φ_d 确实是一个 $A-$ 模同态. 对于任意的 $a \in A$, $l \in L$,

$$\varphi_d(al) = (al)d = a(ld) = a\varphi_d(l)$$

(2) φ 是一个环的反同态. 即 φ 为从 k^{op} 到 $\mathrm{End}_A(L)$ 的环同态. 首先, $\varphi(1) = \varphi_1 = Id_L$. 其次, 对任意的 $d, d^{'}$, 满足 $\varphi_{dd'} = \varphi_{d'} \circ \varphi_d$: 对于任意的 $l \in L$:

$$\varphi_{dd'}(l) = ldd^{'} = \varphi_{d'}(ld) = \varphi_{d'}\varphi_d(l)$$

(3) φ 是一个单同态: 如果 $\varphi(d) = 0$, 即对于任意的 $l \in L = \mathrm{COL}(1)$,

$$\varphi_d(l) = ld = 0$$

根据矩阵 l 的任意性, $d = 0$.

(4) φ 为满同态. 设 $f \in \mathrm{End}_A(L)$ 为 $A-$ 模同态. 注意到,

$$L = AE_{11}, E_{11} \in L$$

其中, E_{11} 为矩阵单位. 记矩阵环 $\mathrm{Mat}_n(k)$ 中第一列为 $[u_1, u_2, \cdots, u_n]^T$, 其他列元素为 0 的矩阵为 $[u_1, u_2, \cdots, u_n]$. 设 $f(E_{11}) = [d_1, d_2, \cdots, d_n]$. 对于任意的 $l = [m_1, m_2, \cdots, m_n] \in L = \mathrm{COL}(1)$,

$$l = [m_1, m_2, \cdots, m_n] = [m_1, m_2, \cdots, m_n]E_{11}$$

因为 f 为 $A-$ 模同态, 故:

$$\begin{aligned} f(l) &= f([m_1, m_2, \cdots, m_n]) \\ &= f([m_1, m_2, \cdots, m_n]E_{11}) \\ &= [m_1, m_2, \cdots, m_n]f(E_{11}) \\ &= [m_1, m_2, \cdots, m_n][d_1, d_2, \cdots, d_n] \\ &= [m_1, m_2, \cdots, m_n]d_1 \\ &= [m_1 d_{1, m_2 d_1, \cdots, m_n d_1}] \\ &= \varphi_{d_1}(m_1, m_2, \cdots, m_n) \\ &= \varphi_{d_1}(l) \end{aligned} \tag{6.6}$$

于是 $f = \varphi_{d_1} \in \mathrm{Im}(\varphi)$.

故 φ 是同构. 即 $k^{op} \cong \mathrm{End}_A(L)$.

□

6.3.3 唯一性定理 (不变量)

为了进一步证明 Artin—Wedderburn 定理的唯一性, 我们需要进一步讨论半单环的结构. 它们是进一步完成 Artin—Wedderburn 定理证明的基础.

定理 6.3.15. *R 是一个半单环, $R = L_1 \oplus L_2 \cdots \oplus L_n = B_1 \oplus B_2 \cdots \oplus B_r$; 其中 L_i 为极小左理想, $B_i = \bigoplus\limits_{L_p \cong L_i} L_p$ 为 L_i 的单直和因子. 对于半单环 R 的结构, 我们有如下性质:*

(1) 单直和因子 B_i 是一个环, 但并非 R 的子环; 同时 B_i 也是 R 的双边理想; 且对于任意的 $i \neq j$, $B_i B_j = \{0\}$.

(2) 对于 R 的任意一个极小左理想 L, 存在 $1 \leq i \leq r$, 使得 $L \cong L_i \subseteq B_i$.

(3) R 中的每一个非零双边理想 D 是单直和因子的直和.

(4) 单直和因子 B_i 是一个单环.

证明. (1) 注意到, 对于任意的 $i \neq j$, $L_i \ncong L_j$. 根据引理(6.3.7), $\mathrm{Hom}_R(L_i, L_j) = \{0\}$, 于是 $L_i L_j = \{0\}$. 从而,

$$B_i B_j = \left(\bigoplus_{L \cong L_i} L \right) \left(\bigoplus_{L' \cong L_j} L' \right) = \bigoplus_{i,j} L_i L_j = \{0\}$$

B_i 是一些极小左理想的直和, 故 B_i 是左理想. 现证 B_i 是右理想:

$$B_i R = B_i(B_1 \oplus B_2 \cdots \oplus B_r) \subseteq B_i B_1 + B_i B_2 + \cdots B_i B_r = B_i B_i \subseteq R B_i \subseteq B_i$$

于是, B_i 是 R 的双边理想. 同时, $B_iB_i \subseteq B_i$ 知 B_i 为一个环. 因为 $1_R = e_1 + e_2 + \cdots + e_r$; $e_j \in B_j$. 对于任意的 $b_i \in B_i$, 我们有:

$$b_i = 1_R \cdot b_i = (e_1 + e_2 + \cdots + e_r)b_i = e_ib_i$$

故 B_i 的单位元是 e_i. 因为 B_i 的单位元与 R 的单位元不同, 故 B_i 是环, 但不是 R 的子环.

(2) 设 L 为 R 的任意一个极小左理想, 则 ${}_RL$ 是一个单模. 根据定理(6.3.8), 存在 $1 \leq i \leq r$, 使得 $L \cong L_i$. 注意到, 如果 $j \neq i$, 则 $B_jL \cong B_jL_i = \{0\}$. 于是,

$$L = RL = (B_1 \oplus B_2 \cdots \oplus B_r)L \subseteq B_1L + B_2L + \cdots + B_rL = B_iL \subseteq B_iR \subseteq B_i$$

(3) D 是 R 的非零双边理想, 首先 D 是一个左理想, 因为 R 是半单环, 所以 D 至少包含一个极小左理想, 记为 L. 根据 (2), 存在 $1 \leq i \leq r$, 使得 $L \cong L_i$. 令 $B_i = \bigoplus\limits_{L_p \cong L_i} L_p$. 断言, $B_i \subseteq D$: 设 $L^{'}$ 为包含在 B_i 的任意一个极小左理想, $L^{'} \cong L_i \cong L$. 根据引理(6.3.7): 存在 $b^{'} \in L^{'}$, 使得 $L^{'} \cong Lb^{'}$. 因为 $L \subset D$, D 为右理想. 故:

$$L^{'} = Lb^{'} \subseteq LL^{'} \subseteq DR \subseteq D$$

即 D 包含 B_i 中的任意极小左理想, 而这些极小左理想均与 L_i 同构. 而 B_i 正是由这些极小左理想生成的. 故 $B_i \subseteq D$. 令

$$B_I = \bigoplus_i B_i; B_i \subseteq D$$

$$B_J = \bigoplus_j B_j; B_j \nsubseteq D$$

根据直和的遗传性(2.2.4),

$$D = B_I \bigoplus (D \cap B_J)$$

其中, $D \cap B_J = \{0\}$. 否则存在极小左理想 $L_j \subseteq D$, 类似上述推论得, B_J 中所有极小左理想都属于 D, B_J 由这些极小左理想生成, 故 $B_J \subseteq D$. 这与 B_J 的选取矛盾. 于是 $D = B_I = \bigoplus\limits_i B_i$.

(4) 只需要注意到, B_i 中的左 (右) 理想也是 R 中的左 (右) 理想. 设 L 是 B_i 的左理想, 则对于任意的 $a = \sum\limits_j a_j \in R$, 其中 $a_j \in B_j$; $b_i \in L$, 注意到, $B_iB_j = \{0\}$(任意$i \neq j$) 我们有

$$ab_i = (a_1 + a_2 + \cdots + a_r) = a_ib_i \in L$$

于是 L 是 R 的左理想. 同理, 对于右理想也类似. 故 B_i 的非零双边理想是 R 的非零双边理想. 根据 (3), B_i 的双边理想是单直和因子的直和. B_i 是单直和因子, 且单直和因子互不相交, 故 B_i 的双边理想只能是本身. 即 B_i 是单环.

□

定理 6.3.16 (Artin—Wedderburn 定理 II). *R 是半单环, 当且仅当存在有限个除环 $k_1, k_2, \cdots, k_r$, 使得*

$$R \cong \prod_{i=1}^{r} \mathrm{Mat}_{n_i}(k_i)$$

其中除环 k_i, 除环的个数 r, 以及矩阵环的阶数 n_i 都由 R 唯一决定.

证明. R 是半单环, $R = B_1 \oplus B_2 \cdots \oplus B_r$ 为关于极小左理想直和分解 $R = L_1 \oplus L_2 \cdots \oplus L_n$ 的单直和分解. 根据 Artin—Wedderburn 定理 (I)(6.3.11), 当且仅当存在有限个除环 $k_1, k_2, \cdots, k_s$, 使得

$$R \cong \prod_{i=1}^{s} \mathrm{Mat}_{n_i}(k_i)$$

其中, $k_i \cong (\mathrm{End}_R(L_i))^{op}$.

(1) **除环的个数 r 由半单环 R 的单直和因子完全决定.** 根据 Schur 引理(6.3.6),

$$\mathrm{End}_R(L_i)$$

是除环. 根据事实(2), 除环的反环为除环; 且根据性质(6.1.5), 除环上的矩阵环是单环, **所以 $\mathrm{Mat}_{n_i}(k_i)$ 是单环. 根据环范畴中直和的性质, 单环 $\mathrm{Mat}_{n_i}(k_i)$ 可嵌入到 $R = \prod_{i=1}^{r} \mathrm{Mat}_{n_i}(k_i)$ 中成为 R 的一个双边理想**. 根据定理(6.3.15), 半单环 R 的双边理想是一些单直和因子 $B_i (1 \leq i \leq r)$ 的直和. 又因为 $\mathrm{Mat}_{n_i}(k_i)$ 是单环, 于是, 存在 $1 \leq k \leq r$, 使得 $\mathrm{Mat}_{n_i}(k_i) = B_k$, 否则 $\mathrm{Mat}_{n_i}(k_i)$ 将含有 R 的双边理想. 故除环的个数等于单直和因子的个数, 即 $r = s$.

(2) **除环以及除环上矩阵环的阶数由半单环 R 决定:** 我们只需证明, 如果存在除环 k, k', 使得 $\mathrm{Mat}_n(k) \cong \mathrm{Mat}_{n'}(k')$, 则 $n = n'$, $k = k'$. 根据性质(6.1.3), $1 \leq \mathrm{COL}(l) (l \leq n)$ 是 $\mathrm{Mat}_n(k)$ 的极小左理想, 且相互同构与 COL(1). 于是 $\mathrm{COL}(l)$ 为 $\mathrm{Mat}_n(k)-$ 单模. 故存在如下关于 $\mathrm{Mat}_n(k)-$ 正则模的合成序列:

$$(0) \subsetneq \mathrm{COL}(1) \subsetneq \cdots \subsetneq \mathrm{COL}(1) \oplus \mathrm{COL}(2) \cdots \oplus \mathrm{COL}(n) = \mathrm{Mat}_n(k)$$

根据 Jordan—Holder 定理(1.4.7), 同构的有限长度模具有等价的合成序列, 且合成序列长度以及因子模为一组不变量. 故 $\mathrm{Mat}_n(k)-$ 正则模与 $\mathrm{Mat}_{n'}(k')-$ 正则模的合成序列等价. 故合成序列长度相等, $n = n'$, 即矩阵环的阶数相等. 然而, 对于任意的 $1 \leq l \leq n$ 有:

$$\mathrm{COL}(l) \cong \mathrm{COL}(1)$$

于是, 除环 $k \cong k'$. 这是因为: 根据推论(6.3.14),

$$k \cong \mathrm{End}_B(L)^{op} \cong \mathrm{End}_{B'}(L')^{op}$$

其中 B 和 $B^{'}$ 分别是 $\mathrm{Mat}_n(k)$ 与 $\mathrm{Mat}_{n'}(k^{'})$ 中关于唯一极小左理想 (同构意义下)L 及 $L^{'}$ 的单直和分量. 而 $L \cong L^{'} \cong \mathrm{COL}(1)$.

□

注 68. 半单环 kG 的单直和因子分解也是矩阵环的直积分解:
R 是一个半单环, $R = L_1 \oplus L_2 \cdots \oplus L_n = B_1 \oplus B_2 \cdots \oplus B_r$; 其中 L_i 为极小左理想, $B_i = \bigoplus\limits_{L_p \cong L_i} L_p$ 为的单直和因子.

(1) 事实上, 有限直和与直积在加法范畴中是一致的. Abel 群范畴, 模范畴都是加性范畴, 但一般的群范畴, 交换环范畴不是加法范畴. Artin—Wedderburn 定理 II 说明了对于一类特殊的环—半单环而言, 单直和因子也是单直积因子.(这里的" 单" 分别强调的是" 单模" 和" 单环")

(2) R 是一个半单环, R 的单直和因子 B_i 不依赖半单环 R 的极小左理想分解, 而由半单环 R 唯一决定. 根据 Artin—Wedderburn 定理 II(6.3.16)可知, 存在有限个除环 $k_1, k_2, \cdots, k_r$, 使得

$$R \cong \prod_{i=1}^{r} \mathrm{Mat}_{n_i}(k_i)$$

事实上, Artin—Wedderburn 定理证明中可知, $B_i \cong \mathrm{Mat}_{n_i}(k_i)$. 于是,

$$R \cong \prod_{i=1}^{r} \mathrm{Mat}_{n_i}(k_i) = R \cong \bigoplus_{i=1}^{r} \mathrm{Mat}_{n_i}(k_i) = \bigoplus_{i=1}^{r} B_i$$

具体地说, 半单环 R 的每一个单直和因子 B_i 由半单环 R 极小左理想直和分解中同构于 L_i 的极小左理想生成, 而 L_i 对应于一个除环 $\mathrm{End}_k(L_i)$, $\mathrm{End}_R(B_i) \cong \mathrm{Mat}_{n_i}(\mathrm{End}_k(L_i))$, 故 B_i 唯一决定一个除环上的矩阵环.

6.3.4 Molien 定理及其推论

下面, 我们给出 Artin—Wedderburn 定理的一些推论, 它们是有限群复表示研究的基础.

定理 6.3.17 (Molien 定理). *G 是一个有限群, k 为代数闭域. $\mathrm{Char}\, k \nmid |G|$, 则群代数 kG 为域 k 上有限个矩阵环的乘积.*

$$kG \cong \mathrm{Mat}_{n_1}(k) \times \mathrm{Mat}_{n_2}(k) \times \cdots \times \mathrm{Mat}_{n_r}(k)$$

证明. 根据 Maschke 定理(2.3.20), kG 为一个半单环. 于是 kG 可以分解为极小左理想的直和:

$$kG = L_1 \oplus L_2 \cdots \oplus L_n$$

根据 Artin—Wedderburn 定理及证明过程 (6.3.11), 存在有限个除环 $D_1, D_2, \cdots, D_r$, 使得

$$kG \cong \prod_{i=1}^{r} \mathrm{Mat}_{n_i}(D_i)$$

且 $D_i \cong (\mathrm{End}_{kG}(L_i))^{op}$, 其中 L_i 第 i 个单直和因子 B_i 的构成极小左理想, 由注记(68), $B_i \cong \mathrm{Mat}_{n_i}(D_i)$. 现断言: $D \cong (\mathrm{End}_{kG}(L_i))^{op} \cong k$. 下面不妨省略下标, 即证 $D \cong k$.

(1) 首先, $D \cong (\mathrm{End}_{kG}(L))^{op} \subseteq (\mathrm{End}_k(L))^{op}$. 这是因为, 对于任意的 $f \in (\mathrm{End}_{kG}(L))^{op}$, f 为 $kG-$ 模同态. 当然, f 也是 $k-$ 模同态. 即 $f \in (\mathrm{End}_k(L))^{op}$.

(2) $k \subseteq \mathrm{Z}(D)$. 对 $a \in k$, 考虑左平移:

$$\varphi_a : L \longmapsto L$$

$$u \longmapsto au$$

容易验证, φ_a 是 $kG-$ 模同态, 即 $\varphi_a \in D$. 现断言 $\varphi_a \in \mathrm{Z}(D)$. 任取 $f \in (\mathrm{End}_k(L))^{op}$, 对于任意的 $u \in L$, 因为 f 也是 $k-$ 模同态, 故

$$f\varphi_a(u) = f(au) = af(u) = \varphi_a(f(u))$$

于是 $f\varphi_a = \varphi_a f$. 即 $\varphi_a \in \mathrm{Z}(D)$. 注意到, 左平移作用是忠实的. 故

$$k \cong \{\varphi_a : L \longmapsto L\} \subseteq \mathrm{Z}(D)$$

于是 $k \subseteq \mathrm{Z}(D)$.

(3) 对于任意的 $\delta \in D$, $k(\delta)$ 为一个域. 因为 $k \subseteq \mathrm{Z}(D)$, 从而 δ 可域 k 中元素交换. 于是在域 k 上添加元素 δ 得到的扩环 $k[\delta]$ 是除环, 因为可交换, 从而是一个域.

(4) $D = k$. 因为 $D = (\mathrm{End}_{kG}(L))^{op}$ 作为为域 k 上的左向量空间是有限维的 (群 G 是有限群). 于是,

$$\infty > [D : k] = [D : k(\delta)][k(\delta) : k]$$

从而 $[k(\delta) : k] \leq \infty$. 即域 $k(\delta)$ 为域 k 的有限扩张. 根据定理(2.6.5)有限扩张都是代数扩张, 从而 $k(\delta)$ 是域 k 的代数扩张. 从而 δ 是域 k 上的代数元. 因为 k 是代数闭域, 所有 $\delta \in k$. 于是 $D = k$.

从而,

$$kG \cong \mathrm{Mat}_{n_1}(k) \times \mathrm{Mat}_{n_2}(k) \times \cdots \times \mathrm{Mat}_{n_r}(k)$$

□

推论 6.3.18. *G 是有限群, L_i 为半单群代数 $\mathbb{C}G$ 的极小左理想, 则*

$$\mathbb{C}G = B_1 \oplus B_2 \oplus \cdots \oplus B_r; B_i = \bigoplus_{L_p \cong L_i} L_p$$

如果 $\dim_{\mathbb{C}}(L_i) = n_i$, 则 $B_i \cong \mathrm{Mat}_{n_i}(\mathbb{C})$, 且 B_i 是 n_i 个同构于极小左理想 L_i 的直和.

证明. 因为 $\mathbb{C}$ 是代数闭域. 根据 Moilen 定理(6.3.17):

$$\mathbb{C}G \cong \prod_{i=1}^{n} \mathrm{Mat}_{n_i}(\mathbb{C})$$

根据 Artin—Wedderburn 定理 II(6.3.16)证明和注记(68)知, 单直和因子分解也是矩阵环的直积分解, 且 $\mathrm{Mat}_{n_i}(\mathbb{C}) \cong B_i$. 两侧取维数,

$$n_i^2 = \dim_{\mathbb{C}}\left(\mathrm{Mat}_{n_i}(\mathbb{C})\right) = \dim_{\mathbb{C}} B_i = \dim_{\mathbb{C}}\left(\bigoplus_{L_p \cong L_i} L_p\right) = \sum_{L_p \cong L_i} \dim_{\mathbb{C}}(L_i) = n_i d$$

从而 $d_i = n_i$. 其中 d 是第 i 个单直和因子 B_i 同构于极小左理想 L_i 的直和.

□

推论 6.3.19. *G 是一个有限群, k 为代数闭域, $\mathrm{Char}\, k \nmid |G|$, $kG = \bigoplus_{i=1}^{n} L_i$, 令 $B_i = \bigoplus_{L_p \cong L_i} L_p$, 则*

$$|G| = n_1^2 + n_2^2 + \cdots + n_1^2$$

其中 n_i 为第 i 个单直和分量 B_i 对应的矩阵阶数 ($B_i \cong \mathrm{Mat}_{n_i}(k_i)$). 更一般的, 我们可以令 $n_1 = 1$.

证明. 根据 Molien 定理(6.3.17), 群代数 kG 为域 k 上有限个矩阵环的乘积.

$$kG \cong \mathrm{Mat}_{n_1}(k) \times \mathrm{Mat}_{n_2}(k) \times \cdots \times \mathrm{Mat}_{n_r}(k)$$

于是, 两边同时取维数:

$$\begin{aligned} |G| &= \dim_k(kG) \\ &= \dim_k\left(\prod_{i=1}^{r} \mathrm{Mat}_{n_i}(k)\right) \\ &= \sum_{i=1}^{r} n_i^2 \end{aligned}$$

特别地, 根据例子(6.3.9)我们知道对于群代数 kG, 存在唯一一个极小左理想 L 同构于主 $kG-$ 模:

$$V_0(k)$$

而 $\dim_k(V_0(k)) = 1 = \dim_L$, 于是 $\dim_k B = \dim_k L = 1$, 即总存在某个 i, $n_i = 1$. 故不妨令 $n_1 = 1$. □

注 69. 事实上, 根据特征标计算可知, $n_i \mid |G|$. 上述推论给出了寻找代数闭域 k 上群代数 kG 的所有单直和因子的方法.

关于半单环 $\mathbb{C}G$ 的单直和因子的个数 m, 我们有一个群论的解释.

定义 6.3.20. G 是一个有限群, $C_1, C_2, \cdots, C_r$ 为共轭类 (conjugacy classes), 则对于每一个共轭类 C_j, 定义**类和 (class sum)**:

$$z_j = \sum_{g \in C_j} g \in \mathbb{C}G$$

引理 6.3.21. *G 是有限群, c 为群 G 共轭类的个数, 则*

$$c = \dim_{\mathbb{C}G}(\mathrm{Z}(\mathbb{C}G))$$

其中, $\mathrm{Z}(\mathbb{C}G)$ 为群代数 $\mathbb{C}G$) 的中心. 并且, 作为线性空间, $\mathrm{Z}(\mathbb{C}G)$ 的一组基由所有的类和 z_j 组成.

证明. 设有限群 G 的共轭类为 $\{C_j\}_{j=1}^r$, $z_j = \sum\limits_{g \in C_j} g$ 为共轭类 C_j 的类和.

(1) $z_j \in \mathrm{Z}(\mathbb{C}G)$.

对于任意的 $h \in G$, 考察

$$hz_jh^{-1} = h(\sum_{g \in C_j} g)h^{-1} = \sum_{g \in C_j} hgh^{-1} = z^j \quad \text{(共轭类的性质)}$$

故 $hz_j = z_jh$, 即 $z_j \in \mathrm{Z}(\mathbb{C}G)$.

(2) $z_1, z_2, \cdots, z_r$ 为 $Z(\mathbb{C}G)$ 的一组基.

(a) $z_1, z_2, \cdots, z_r$ 线性无关.

对于任意的 $j \neq l$, $z_j = \sum\limits_{g \in C_j} g$ 和 $z_l = \sum\limits_{g \in C_l} g$ 没有公共的组成成分 (共轭类互不相交). 故如果存在 $c_1, c_2, \cdots, c_r \in \mathbb{C}$, 使得

$$c_1z_1 + c_2z_2 + \cdots + c_rz_r = 0$$

注意到, 上述式子正是群代数 $\mathbb{C}G$ 的一组基 G 的线性组合. 于是对任意的 $1 \leq i \leq r$, $c_i = 0$.

(b) 对于任意的 $u \in \sum\limits_{g \in G} a_g g \in \mathrm{Z}(\mathbb{C}G)$, u 都可以被 $z_1, z_2, \cdots, z_r$ 线性线性表示.

对于任意的 $h \in G$, 注意到

$$\sum_{g \in G} a_g g = u = huh^{-1} = h(\sum_{g \in G} a_g g)h^{-1} = \sum_{g \in G} a_g hgh^{-1} = \sum_{g \in G} a_{hgh^{-1}} g$$

故对任意的 $g \in G$, $a_{ghg^{-1}} = a_g$. 如果 g_1, g_2 在群 G 相同的共轭类当中, 则系数相等. 于是, 记第 j 个共轭类对应的系数为 c_j, 则

$$u = \sum_{g \in G} a_g g = \sum_{j=1}^{r} c_j z_j$$

□

注 70. 借此, 我们对群代数的定义进行回顾, G 是一个有限群, k 是一个域, 记 kG 为以群 G 中的元素为基生成的域 k 上的线性空间, 其加法和乘法如下: 对于任意的 $\sum\limits_{g \in G} a_g g, \sum\limits_{g \in G} b_g g \in kG$, $c \in \mathbb{C}$:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

$$c(\sum_{g \in G} a_g g) = \sum_{g \in G} (c a_g) g$$

先定义乘法, 使得 kG 为域 k 上的群代数.

$$(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{g \in G} \left(\sum_{xy = g} a_x b_y \right) g$$

且乘法与数乘可任意交换:

$$c(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{g \in G} ((c a_g) g)\,(\sum_{g \in G} b_g g) = \sum_{g \in G} (a_g g)(\sum_{g \in G} ((c b_g) g)$$

定理 6.3.22 (单直和分量的个数等于群的共轭类数). *G 是一个有限群, 则复群代数 $\mathbb{C}G$ 单直和分量的个数 r 等于群 G 的共轭类个数 $c = \dim_{\mathbb{C}}(\mathrm{Z}(\mathbb{C}G))$.*

证明. 注意到 $\mathrm{Z}(\mathrm{Mat}_{n_i}(\mathbb{C})) = \mathrm{S}(n_i, \mathbb{C})$. 根据 Molien 定理(6.3.17),

$$\mathbb{C}G \cong \prod_{i=1}^{n} \mathrm{Mat}_{n_i}(\mathbb{C})$$

且容易知道:

$$\mathrm{Z}(\mathbb{C}G) = \mathrm{Z}\left(\prod_{i=1}^{n} \mathrm{Mat}_{n_i}(\mathbb{C}) \right) = \prod_{i=1}^{r} \mathrm{Z}(\mathrm{Mat}_{n_i}(\mathbb{C})) = \prod_{i=1}^{r} \mathrm{S}(n_i, \mathbb{C})$$

于是,

$$\begin{aligned} c = \dim_{\mathbb{C}} \mathrm{Z}(\mathbb{C}G) &= \dim_{\mathbb{C}} \left(\mathrm{Z}(\prod_{i=1}^{r} \mathrm{Mat}_{n_i}(\mathbb{C})) \right) \\ &= \dim_{\mathbb{C}} \left(\prod_{i=1}^{r} \mathrm{Z}(\mathrm{Mat}_{n_i}(\mathbb{C})) \right) \\ &= \dim_{\mathbb{C}} \left(\prod_{i=1}^{r} \mathrm{S}(n_i, \mathbb{C}) \right) \end{aligned}$$

而注意到

$$\dim_{\mathbb{C}}\left(\prod_{i=1}^{r}\mathrm{S}(n_i,\mathbb{C})\right)=\sum_{i=1}^{r}\dim_{\mathbb{C}}(\mathrm{S}(n_i,\mathbb{C}))=\sum_{i=1}^{r}1=r$$

于是,

$$c=\dim_{\mathbb{C}}(\mathrm{Z}(\mathbb{C}G))=r$$

□

下面进一步阐述从 $kG-$ 模的研究反馈到 k 表示的一些结果.

定义 6.3.23. k 为一个域, V/k 是域 k 上的线性空间. $\sigma:G\mapsto \mathrm{GL}(V)$ 为一个 k 表示, 称表示 σ 为**不可约表示 (irreducible representation)**, 如果 σ 决定 $kG-$ 模 V^{σ} 为不可约模.

例 6.3.24. k 是一个域, G 为一个群, 一维 k 表示 $\lambda:G\mapsto k^{\times}$ 为不可约表示, 因为相应的 $kG-$ 模 $V_0(k)$ 维数为 1, 为不可约模.

定义 6.3.25. k 是一个域, G 为一个群, V/k 是域 k 上的线性空间, 称表示 $\sigma:G\mapsto \mathrm{GL}(V)$ 是**线性表示 (linear representation)**, 如果表示的次数(6.2.1)为:

$$\deg(\sigma)=\dim_k(V)=1$$

Artin—Wedderburn 定理用到有限 Abel 群的复表示中可得不可约表示都是线性表示.

定理 6.3.26 (有限 Abel 群不可约复表示是线性表示). *G 为有限 Abel 群, G 的不可约复表示都是线性表示.*

证明. 根据 Artin—Wedderburn 定理 II(6.3.16)的证明过程及其注释, 群代数 $\mathbb{C}G$ 的单直和因子分解也是矩阵环的直积分解:

$$\mathbb{C}G=B_1\oplus B_2\oplus\cdots\oplus B_t=\mathrm{Mat}_{n_1}(\mathbb{C})\times\mathrm{Mat}_{n_2}(\mathbb{C})\times\cdots\times\mathrm{Mat}_{n_t}(\mathbb{C})$$

其中, $B_i\cong\mathrm{Mat}_{n_i}(k_i)$, k_i 是除环. 因为 G 为 Abel 群, 故 $n_i=1$, 即:

$$\mathbb{C}G\cong\mathbb{C}\times\mathbb{C}\times\cdots\times\mathbb{C}$$

即第 i 个单直和分量 $B_i\cong\mathbb{C}$. 因为 $\dim_{\mathbb{C}}(B_i)=\dim_{\mathbb{C}}\left(\bigoplus\limits_{L_p\cong L_i}L_p\right)=1$, 故 $\mathbb{C}G$ 的互不同构的极小左理想均同构于 $L_i\cong\mathbb{C}$, 也就是说 $\mathbb{C}G$ 在同构意义下仅有一个极小左理想 L, $L\cong\mathbb{C}$. 然而, G 的不可约复表示 σ 确定一个 $\mathbb{C}G-$ 模, 每一个不可约 $\mathbb{C}G-$ 模同构于极小左理想 $L\cong\mathbb{C}$, 于是 $\deg(\sigma)=\dim_{\mathbb{C}}(L)=\dim_{\mathbb{C}}(\mathbb{C})=1$, 即不可约复表示都是线性的. □

定理 6.3.27 (构造特征标表的基本定理). *G 为有限群, G 的不可约复表示的个数 ($\mathbb{C}G-$单模的个数) 等于群 G 共轭类的个数.*

证明. 不可约复表示的个数 $=\mathbb{C}G-$ 单模的个数 $=\mathbb{C}G$ 互不同构的极小左理想的个数 = 单直和因子的个数. 根据定理(6.3.22)知, 单直和因子的个数 $=\dim_{\mathbb{C}}(\mathrm{Z}(\mathbb{C}G))=$ 共轭类的个数. 即有不可约复表示的个数等于群 G 的共轭类数. □

例 6.3.28. 下面, 我们利用 Molien 定理及其推论, 给出群代数做直和分解的例子:

(1) $G=S_3$, $k=\mathbb{C}$. 考虑 G 的复表示: $|S_3|=6$. 因为 $\mathbb{C}$ 是代数闭域, 根据 Molien 定理(6.3.17), 群代数 $\mathbb{C}G$ 为域 $\mathbb{C}$ 上有限个矩阵环的乘积.

$$\mathbb{C}G\cong \mathrm{Mat}_{n_1}(\mathbb{C})\times \mathrm{Mat}_{n_2}(\mathbb{C})\times\cdots\times \mathrm{Mat}_{n_r}(\mathbb{C})$$

$\dim_{\mathbb{C}}(\mathbb{C}G)=6$. S_3 有三个共轭类, 这是因为根据推论(6.3.19),

$$|G|=1+n_2^2+n_3^2=6$$

因为 n_2,n_3 均为自然数, 则仅有解 $n_2=1$, $n_3=2$, 从而

$$\mathbb{C}S_3\cong \mathbb{C}\times\mathbb{C}\times \mathrm{Mat}_n(\mathbb{C})$$

事实上, n 阶置换群 S_n 的共轭类个数等于不同循环结构 (cycle structures) 的个数, 具体可参见 Rotman, Advance Modern Algebra, Theorem A-4.7 in Part 1.

(2) $G=Q_8$ 为八元数群, $k=\mathbb{C}$. 考虑 G 的复表示: 根据 Molien 定理(6.3.17), 群代数 $\mathbb{C}G$ 为域 $\mathbb{C}$ 上有限个矩阵环的乘积.

$$\mathbb{C}G\cong \mathrm{Mat}_{n_1}(\mathbb{C})\times \mathrm{Mat}_{n_2}(\mathbb{C})\times\cdots\times \mathrm{Mat}_{n_r}(\mathbb{C})$$

根据推论(6.3.19)

$$|Q_8|=8=1+n_2^2+\cdots+n_r^2$$

因为 n_i 均为自然数, 故方程的解仅有以下两种情况:
情况一: 对任意的 $1\le i\le 8$, $n_i=1$, 此时有 $\mathbb{C}Q_8$ 为交换环, 而群代数 CG 交换当且仅当群 G 交换, 于是 Q_8 交换, 八元数群不是交换群, 从而矛盾.
情况二: $n_2=n_3=n_4=1$, $n_5=2$. 此时,

$$\mathbb{C}Q_8\cong \mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times \mathrm{Mat}_2(\mathbb{C})$$

从而, 根据定理(6.3.22), 单直和因子的个数等于共轭类的个数, 则八元数群 Q_8 有五个共轭类:

$$\{1\},\{\overline{1}\},\{i,\overline{i}\},\{j,\overline{j}\},\{k,\overline{k}\}$$

6.3.5 Jordan—Chevalley 稠密定理

Artin—Wedderburn 定理在表示论当中起着重要的作用, 它不但揭示了半单环的结构, 而且给出了刻画半单环的一组完全不变量, 完成了半单环的分类. 半单环是 Artin 环 (因为半单环满足 DCC 和 ACC 两个链条件), 而 Artin 环都是 Noether 环 (参考 Rotman, Advanced Modern Algebra Part2, Page139,Theorem C-2.21, Hopkins–Levitzki), 因此半单环是某类特殊的 Artin 环 (可表示成有限个极小左理想的直和).

1930 年, Jordan—Chevalley 对于某类非 Artin 环推广了 Artin—Wedderburn 定理. 这类环是本原环. 关于本原环, Artin—Wedderburn 定理的推广成为 Jordan—Chevalley 稠密定理. Jordan—Chevalley 稠密定理在非交换代数, 非交换几何几何, 辛几何, 李理论等分支起着重要的作用.

定义 6.3.29. 称一个环 R 为**左本原的 (left primitive)**, 如果存在一个左 R-单模 S, 单模 S 是**忠实的 (faithful)**: 如果存在 $r \in R$, 使得 $rS = \{0\}$, 则 $r = 0$.

定理 6.3.30 (Jordan—Chevalley 稠密定理). *R 是一个左本原环, S 为左 $R-$ 忠实单模, 则以下结论成立:*

(1) R 为交换环, 则 R 为域.

(2) R 为左 Artin 环, 则 R 为单环.

(3) 左 $R-$ 忠实单模 S 的模自同态环 $k = \mathrm{End}_R(S)$ 为一个除环.

(4) 若 R 为左 Artin 环, 则:

$$R \cong \mathrm{Mat}_n(k) = \mathrm{Mat}_n(\mathrm{End}_R(S))$$

(5) 若 R 不是左 Artin 环, 则对于任意的 $n \geq 0$, 存在 R 的子环 R_n, 使得:

$$R_n \cong \mathrm{Mat}_n(k) = \mathrm{Mat}_n(\mathrm{End}_R(S))$$

证明. 参考 Lam 的 <A First Course in Noncommutative Rings>, pp191-193. □

注 71. Artin—Wedderburn 定理推动了许多代数学领域的研究, 其中影响最大的两个领域是: 除环的结构刻画与有限维代数的结构与表示. 对于有限维代数表示论, 得益于 Maschke 定理(2.3.20)和 Molien 定理(6.3.17) . Artin—Wedderburn 定理可以运用到有限群的常表示(6.2.6). 然而, 当群代数不是半单代数时, 有限群的模表示自然的被提出. 例如, G 是有限可解群, 则 G 中的极小正规子群为 $\mathbb{F}_p$(p 为素数) 上的线性空间. 考虑共轭作用 $G \curvearrowright N$, 则 N 是一个 $\mathbb{F}_pG-$ 模. 模表示在分类有限单群中广泛运用. 为了研究模表示, Brauer 发现了比常表示中不可约模 (irreducible module) 更为重要的结构块 (block)—不可分解模 (indecomposable module).

定义 6.3.31. R 是一个环, 称 $R-$ 模 M 为不可分解模 (indecomposable module), 如果 $M \neq \{0\}$, 且不存在非零 $R-$ 模 A, B 使得 $M = A \oplus B$.

注 72. 在有限群的常表示下, 不可约模等价于不可分解模. 在有限群的模表示中, 不可分解模更为适用.

6.3.6 Krull-Schedmit 定理

Krull-Schedmit 定理体现了不可分解模的重要性在于, 有限长度模关于不可分解模的直和分解是唯一的. Krull-Schedmit 定理是重要的直和分解唯一性定理, 有兴趣的读者把此定理与 Jordan—Holder 定理(1.4.7)进行比较.

定理 6.3.32 (Krull-Schedmit 定理). *R 为一个环, A 为左 $R-$ 模. A 满足 ACC 和 DCC 链条件, 并且存在如下直和分解:*

$$A = H_1 \oplus H_2 \oplus \cdots \oplus H_s = K_1 \oplus K_2 \oplus \cdots \oplus K_t$$

其中, H_i 和 K_j 均为不可分解模, 则 $s = t$; 且在不计次序的意义下, $H_i \cong K_i$. 更重要的是, 存在一个替换性质 (replacement property): 任给 $1 \leq r \leq s$, 在适当调整顺序后, 可选择如下结构块对 A 进行分解:

$$A = H_1 \oplus H_2 \oplus \cdots \oplus H_r \oplus K_{r+1} \oplus \cdots \oplus K_s$$

注 73. Krull—Schedmit 定理给出了有限生成 Abel 群基定理(4.1.14)的唯一性定理—基本定理(4.2.8). 这是因为 $p-$ 准素循环群和无限循环群都是不可分解 $\mathbb{Z}-$ 模.

下面, 我们把有限群模表示的不可分解模与常表示的不可约模进行比较如下: k 是一个域, G 是一个有限群.

(1) kG 是半单环时, $kG-$ 模是半单模, 根据定理(6.3.8), 半单环上的不可约模对应于一个极小左理想, 从而 kG 上在同构意义下仅有有限多个互不同构的不可约模 (此时, 不可分解模和不可约模等价).

(2) kG 不是半单环时, kG 上可以存在无限多个互不同构的不可分解模. 例如, 当 k 为代数闭域, $\operatorname{Char} k = 2$, $G = \mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$ 或者 $G = A_4$ 时对应的群代数 $k\mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$, kA_4 上均存在无限多个互不同构的不可分解模.

定义 6.3.33. 称域 k 上的有限维 $k-$ 代数 R 为**有限型表示的 (finite representation type)**, 如果 R 上的模在同构意义下, 仅存在有限多个互不同构的有限维不可分解模.

特别地, 有限群的常表示是有限型表示. D.G.Higman 对有限群刻画了有限型表示.

定理 6.3.34 (D.G.Higman). *G 是一个有限群, 对于任意的域 k, 群代数 kG 是有限型表示当且仅当, G 的所有 Sylow $p-$ 子群是循环群.*

证明. 参考 Curtis–Reiner <Representation Theory of Finite Groups and Associative Algebras>, Page 431. □

1950 年, 关于不可分解模的 **Brauer—Thrall 猜想**被提出: R 是一个环, R 不是有限型表示的, 则 Brauer—Thrall 猜想是指:

(1) R 上的不可分解模的维数是否无界 (unbounded)?

(2) 对于 R 上的互不同构的不可分解模的维数 n_i, 是否存在严格的递增序列:

$$n_1 \leq n_2 \leq \cdots$$

迄今为止, Brauer—Thrall 猜想的两个问题都得到了完美的回答, 在解决这个猜想的过程当中, 人们发掘了一些在代数表示论当中极为重要的工具: 几乎可裂序列, 箭图代数, 邓肯图等. 这些工具在有限维代数表示论, 复半单李代数的分类及范畴论当中都非常重要. 下面, 简单列出 Brauer—Thrall 定理证明中的主要过程:

(A) Brauer—Thrall 中的问题 (1):

(1) 1968 年, Roiter 解决了问题 (1). 随后 Grabriel 引入了图论的方法 (graph–theoretic methods): 把有限维代数与某种定向图 (quiver) 联系起来. Grabriel 证明了: 一个连通的定向图 (connected quiver) 存在有限多个互不同构的有限维表示, 当且仅当这个箭图 (quiver) 是邓肯图 (Dykin diagram) 中的

$$A_n, D_n, E_6, E_7, E_8$$

五种类型之一.

(2) Dykin 图是一种用于分类复数域上单李代数的多重图 (multigraphs).

(3) 进一步, Gabriel 的结果可以用左遗传 (left hereditary)$k-$ 代数 (左理想作为正则模是投射模) 重新描述与证明.

(4) Dlab 和 Ringel 把 Gabriel 的结果从左遗传代数推广到了有所的 Dykin 图.

(B) Brauer—Thrall 中的问题 (2):

(1) Bautistu, Gabriel 以及 Roiter 和 Salmeron 共同给出了代数闭域上的所有有限维代数的结果.

(2) Auslander 与 Reiten 创造了一套理论几乎可裂序列 (almost split sequences) 和 Auslander—Reiten quivers 解决了问题 (2), 这是研究有限维代数表示论的主要工具.

6.4 李代数简介

我们已经学习了许多种代数结构, 它们大多数都是结合代数. 事实上还存在着许多非结合代数的例子, 其中最重要的就是李代数. 我们将在本节进行李代数的简单介绍, 供有兴趣的读者阅读.

在定义李代数之前, 我们先来介绍导子的概念.

定义 6.4.1. 交换环 k 上的一个**不必结合的 k-代数 (not-necessarily-associative k-algebra)** A 是一个 $k-$ 模配备了二元运算 $A\times A\to A$, 定义为 $(a,b)\mapsto ab$, 满足

(1) 对于任意的 $a,b,c\in A$, 有 $a(b+c)=ab+ac$; $(b+c)a=ba+ca$.

(2) 对于任意的 $u\in k, a\in A$, 有 $ua=au$.

(3) 对于任意的 $u\in k, a,b\in A$, 有 $a(ub)=(au)b=u(ab)$.

A 的一个**导子 (derivation)** 是一个 $k-$ 映射 $d: A\to A$, 满足对任意的 $a,b\in A$, 有

$$d(ab)=(da)b+a(db).$$

事实上, 两个导子的复合不一定是导子. 例如, 如果 $d: A\to A$ 是一个导子, 则 $d^2=d\circ d: A\to A$ 满足等式

$$d^2(fg)=d^2(f)g+2d(f)d(g)+fd^2(g);$$

因此混合项 $2d(f)d(g)$ 将阻碍 d^2 成为一个导子. 然而计算两个导子 d_1,d_2 的复合是有价值的. 假设 A 是一个不必结合的代数, $f,g\in A$, 则:

$$\begin{aligned} d_1d_2(fg) &= d_1[(d_2f)g+f(d_2g)] \\ &= (d_1d_2f)g+(d_2f)(d_1g)+(d_1f)(d_2g)+f(d_1d_2g). \end{aligned}$$

而

$$d_2d_1(fg)=(d_2d_1f)g+(d_1f)(d_2g)+(d_2f)(d_1g)+f(d_2d_1g).$$

如果我们定义 $[d_1,d_2]=d_1d_2-d_2d_1$, 则

$$[d_1,d_2](fg)=([d_1,d_2]f)g+f([d_1,d_2]g);$$

即 $[d_1,d_2]=d_1d_2-d_2d_1$ 为一个导子.

例 6.4.2. 设 k 是一个交换环, 将 $\mathrm{Mat}_n(k)$ 配备**括号运算 (bracket operation)**:

$$[A,B]=AB-BA.$$

显然 A, B 交换当且仅当 $[A, B] = 0$. 容易验证括号运算是非结合的. 然而对于任意的 n 阶矩阵 M, 函数

$$ad_M : \mathrm{Mat}_n(k) \to \mathrm{Mat}_n(k),$$

定义为

$$ad_M : A \to [M, A],$$

是一个导子:

$$[M, [A, B]] = [[M, A]\ B] + [A, [M, B]].$$

读者可自行验证.

定义 6.4.3. 一个**李代数 (Lie algebra)** 指的是域 k 上的线性空间 L 配备了一个双线性运算 $L \times L \to L$, 定义为 $(a, b) \mapsto [a, b]$(称为**括号 (bracket)**), 满足

(1) 对于任意的 $a \in L$, 有 $[a, a] = 0$.

(2) 对于任意的 $a \in L$, 函数 $ad_a : b \mapsto [a, b]$ 是一个导子.

对于任意的 $u, v \in L$, 由双线性性得

$$[u + v, u + v] = [u, u] + [u, v] + [v, u] + [v, v],$$

而 $[a, a] = 0$, 得

$$[u, v] = -[v, u];$$

即括号具有**反交换性 (anticommutative)**. 第二点一般可以写的更为详细. 如果 $b, c \in L$, 那么 ad_a 是一个导子就是说:

$$[a, [b, c]] = [[a, b], c] + [b, [a, c]];$$

由反交换性可得 **Jacobi 恒等式 (Jacobi identity)**: 对于任意的 $a, b, c \in L$, 有

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$$

下面给出一些李代数的例子.

例 6.4.4. (i) 如果 V 是域 k 上的线性空间, 对于任意的 $a, b \in V$, 定义 $[a, b] = 0$. 显然 V 成为一个李代数, 称为**交换 (abelian)** 李代数.

(ii) 在 $\mathbb{R}^3$ 中, 定义 $[u, v] = u \times v$ 为**叉乘 (cross product)**. 容易验证 $\mathbb{R}^3$ 成为一个李代数.

(iii) 李代数 L 的一个**子代数 (subalgebra)** S 是一个子空间在括号下封闭: 如果 $a, b \in S$, 则 $[a, b] \in S$. 容易验证李代数的每个子代数本身都是李代数.

(iv) 如果 k 是一个域, 则 $\mathrm{Mat}_n(k)$ 在括号运算 $[A,B]=AB-BA$ 下成为一个李代数. 通常记为 $\mathrm{GL}(n,k)$. 这个例子十分重要, 因为如果域 k 的特征为 0, 则 k 上的每个有限维李代数同构于 $\mathrm{GL}(n,k)$ 的子代数.

(v) $\mathrm{GL}(n,k)$ 的一个重要子代数为 $\mathrm{SL}(n,k)$, 其由全体迹为 0 的 n 阶矩阵构成.

(vi) 如果 A 为域 k 上的任意李代数, 则:

$$\mathcal{D}(A/k)=\{\text{所有导子 } d:A\to A\}$$

为李代数, 其中李括号运算为 $[d_1,d_2]=d_1d_2-d_2d_1$.

定义 6.4.5. 设 L,L' 为域 k 上的李代数, 称函数 $f:L\to L'$ 为**李代数同态 (Lie homomorphism)**, 如果对于任意的 $a,b\in L$, f 为 $k-$ 线性映射并且满足括号运算:

$$f([a,b])=[fa,fb].$$

定义 6.4.6. 李代数 L 的一个**理想 (ideal)** 是一个子空间 I, 满足对于任意的 $x\in L, a\in I$ 有 $[x,a]\in I$.

尽管李代数不满足交换性, 但其反交换性保证了其每个理想都是双边理想.

一个李代数 L 称为**单代数 (simple)** 如果 $L\neq\{0\}$ 且 L 没有非零的真理想.

定义 6.4.7. 如果 I 是 L 的一个理想, 则**商代数 (quotient)**L/I 是商空间 (将 L 看作线性空间, I 看作其子空间), 括号运算定义为

$$[a+I,b+I]=[a,b]+I.$$

例 6.4.8. (i) 设 $f:L\to L'$ 为李代数同态, 则其**核 (kernel)** 定义为:

$$\ker f=\{a\in L:f(a)=0\}.$$

容易验证 $\ker f$ 为 L 的理想.

自然映射 (natural map)$v:L\to L/I$, 定义为 $a\mapsto a+I$ 为李代数同态, 其核为 I. 因此 L 的子空间是理想当且仅当其为某个李代数同态的核.

(ii) 设 I,J 为李代数 L 的理想, 则

$$IJ=\Big\{\sum_r[i_r,j_r]:i_r\in I,j_r\in J\Big\}.$$

特别地, 记 $L^2=LL$; $L^2=\{0\}$ 当且仅当 L 是交换的.

(iii) 李代数 L 的**导来链 (derived series)** 归纳地定义为:

$$L^{(0)}=L, L^{(n+1)}=(L^{(n)})^2.$$

李代数 L 称为**可解的 (solvable)**, 如果存在某个 $n\geq 0$ 使得 $L^{(n)}=\{0\}$.

(iv) 可归纳地定义李代数 L 的**中心降链 (descending central series)**:

$$L_1 = L, L_{n+1} = LL_n.$$

李代数 L 称为**幂零的 (nilpotent)**, 如果存在某个 $n \geq 0$ 使得 $L_n = \{0\}$.

最后, 我们将不加证明的为读者介绍两个李代数的重要定理. 如果 L 为李代数, $a \in L$, 则 $ad_a : L \to L$, 定义 $ad_a : x \mapsto [a, x]$ 为 L 上的线性变换. 我们称 a 是 **ad-幂零 (ad-nilpotent)** 的, 如果 ad_a 是幂零的, 即存在某个 $m \geq 1$ 使得 $(ad_a)^m = 0$.

定理 6.4.9 (**Engle's Theorem**). *(i) 设 L 是域 k 上的有限维李代数, 则 L 是幂零的当且仅当对于任意的 $a \in L$ 都是 $ad-$ 幂零的.*

(ii) 设 L 为 $\mathrm{GL}(n, k)$ 的李子代数, 其元素 A 都为幂零矩阵. 则 L 可严格上三角化 (对角线元素都为 0); 即存在非奇异矩阵 P 使得对于任意的 $A \in L$, PAP^{-1} 为严格上三角矩阵.

定理 6.4.10 (**Lie's Theorem**). *设 k 为代数闭域, 则 $\mathrm{GL}(n, k)$ 的每个可解子代数 L 可上三角化; 即存在非奇异矩阵 P, 使得对于任意的 $A \in L$, PAP^{-1} 为上三角矩阵.*

6.5 特征标

表示论的一个重要内容就是研究抽象群到非奇异矩阵群的一个同态, 这种同态产生的不变量, 用于研究抽象群的性质. 今天我们将介绍将一个群表示翻译成模的语言, 然后通过模的分类将特征标进行分类, 而特征标又是可以具体到矩阵群中矩阵的对角线之和 (矩阵的迹).

引理 6.5.1. *若 $H \lhd G$ 且 H 和 G/H 都是可解群, 则 G 是可解群.*

证明. 因 G/H 是可解的, 则存在正规列, 其具有素数阶因子群:

$$G/H \geq K_1^* \geq K_2^* \geq \cdots \geq K_m^* = \{1\}$$

由群的对应定理知, 存在 G 的子群 K_i 满足:

$$G \geq K_1 \geq K_2 \geq \cdots \geq K_m = H$$

其中对一切 i, $K_i/H = K_i^*$, $K_{i+1} \lhd K_i$. 根据第三同构定理有, 对一切的 i 我们有:

$$K_i^*/K_{i+1}^* \simeq K_i/k_{i+1}$$

从而, K_i/K_{i+1} 也是素数阶循环群, 而 H 是可解群, 故存在正规列:

$$H \geq H_1 \geq H_2 \geq \cdots \geq H_p = \{1\}$$

具有素数阶因子群, 则把此序列同上述序列结合有:

$$G \geq K_1 \geq \cdots \geq K_m \geq H_1 \geq H_2 \geq \cdots \geq H_p = \{1\}$$

且因子 K_i/K_{i+1} 及 H_i/H_{i+1} 为素数阶循环群, 故 G 可解. □

定理 6.5.2 (Burnside). 阶为 $p^m q^n$ 的每个群 G 是可解群, 其中 p, q 为素数.

注 74. Burnside 定理不能改进到阶为三个不同素因子的群, 例如 A_5, 它的阶为 $60 = 2^2 \times 3 \times 5$. 又 A_5 为单群, 故其不可解.

性质 6.5.3. 如果 G 是非 *Abel* 的有限单群, 则 $\{1\}$ 是大小为素数幂的唯一共轭类.

引理 6.5.4. 上面的性质(6.5.3)蕴含 *Burnside* 定理.

证明. 若 Burnside 定理不成立, 设 G 为最小的" 出界者", 即 $|G|$ 为最小的反例. 若 G 有非平凡正规子群 H, 则 $H \neq \{1\}$, 则 H 和 G/H 都是可解的. 因为它们的阶数都小于 $|G|$(归纳假设), 并且阶的个数都为 $p^i q^j$ 的形式 $(i \leq m, j \leq n)$. 由下面的引理可知 G 是可解的, 与题设矛盾. □

定义 6.5.5. 群 G 的一个**表示 (representation)** 是一个同态 $\sigma : G \to \mathrm{GL}(V)$. 其中, V 是 $\mathbb{C}$ 上的向量空间, σ 的次数是 $\dim(V)$.

注 75. 表示可以翻译成模的语言, 我们可以证明每个 $\sigma : G \to \mathrm{GL}(V)$ 把 V 配置成一个左 $\mathbb{C}G$-模的结构. 反之亦然, 若 $g \in G$, 则 $\sigma(g) : V \to V$ 对 $g \in G$ 和 $v \in V$, 定义标量乘法为:

$$(g.v) = gv = \sigma(g)(V)$$

例 6.5.6. 现证明置换表示, 即 G-集给出一个特殊类型的表示, 一个 G-集对应一个同态 $\pi : G \to S_X$, 其中 S_x 是集合 X 的一切置换构成的对称群. 如果 V 是以 x 为基的复向量空间, 则可以用下面的方式看 $S_X \leq \mathrm{GL}(V)$. X 的每个置换 $\pi(g)$ 是 V 的基的一个置换, 因此它确定 V 上的一个非奇异线性变换. 对于基 X, $\pi(g)$ 的矩阵是一个置换矩阵, 它是把单位矩阵 E 进行交换行 (列) 变换得到的. 于是, 它的每行每列恰有一个元素等于 1, 而其他元素都为 0.

定义 6.5.7. 若 G 是群, 则定义表示:

$$\begin{aligned} \rho : G &\to \mathrm{GL}(\mathbb{C}G) \\ g &\mapsto \rho(g) : h \mapsto gh \end{aligned}$$

这个表示称为**正则表示 (regular representation)**.

定义 6.5.8. 如果 $\sigma : G \to \mathrm{GL}(V)$ 和 $\tau : G \to \mathrm{GL}(W)$ 是群 G 的两个复表示, 则定义他们的和:

$$\sigma + \tau : G \to \mathrm{GL}(V \oplus W)$$
$$g \mapsto (\sigma + \tau)(g) : (v, w) \mapsto (\sigma(g)v, \tau(g)w)$$

用矩阵的语言, 若 $\sigma : G \to \mathrm{GL}(n, \mathbb{C})$ 和 $\tau : G \to \mathrm{GL}(m, \mathbb{C})$, 则:

$$\sigma + \tau : G \longrightarrow \mathrm{GL}(n + m, \mathbb{C})$$

并且如果 $g \in G$, 则 $(\sigma + \tau)(g)$ 是块的直和 $\sigma(g) \oplus \tau(g)$. 即:

$$(\sigma + \tau)(g) = \begin{bmatrix} \sigma(g) & 0 \\ o & \tau(g) \end{bmatrix}$$

定义 6.5.9. 群 G 的一个表示是**不可约的 (irreducible representation)**, 如果对应的 $\mathbb{C}G$-模是单的; 称一个表示 σ 是**可约的 (reducible)**, 如果它是不可约的直和, 即对应的 $\mathbb{C}G$-模是半单的.

引理 6.5.10. *设 R 是左半单环, 并设 $R = L_1 \oplus L_2 \oplus \cdots \oplus L_n = B_1 \oplus B_2 \oplus \cdots \oplus B_m$. 其中, L_j 是对应的极小左理想, B_i 是 R 的单分量, 则有以下结论:*

(1) 每个 B_i 是环, 且是 R 中的双边理想, 当 $i \neq j$ 时, $B_i B_j = \{0\}$.

(2) 如果如果 L 时 R 中的任一极小左理想, 则它不必出现在 R 的给定分解中, 有某个 i 使得 $L \backsimeq L_i$, 且 $L \subseteq B_i$.

(3) R 中的每个双边理想 D 都是若干 B_i 的直和.

(4) 每个 B_i 都是单环.

性质 6.5.11. *(1) 对 $\mathbb{C}G$ 的每个极小左理想 L_i, 存在不可约表示:*

$$\lambda_i : G \to \mathrm{GL}(L_i)$$
$$g \mapsto \lambda_i(g)(u_i) = g.u_i$$

其中, $g \in G$,$u_i \in L_i$. 此外, $\deg(\lambda_i) = n_i = \dim(L_i)$.

(2) 如果对 $g \in G$ 和 $u_i \in B_j$, 定义

$$\tilde{\lambda_i}(g)u_j = \begin{cases} gu_i & j = i \\ 0 & j \neq i \end{cases}$$

则表示 λ_i 扩张为 $\mathbb{C}$-代数映射 $\tilde{\lambda_i} : \mathbb{C}G \longrightarrow \mathbb{C}G$

证明. (1) 因 L_i 是 $\mathbb{C}G$ 的左理想, 每个 G 的正则表示限制在 L_i 上, 从而得到对应的表示 λ_i. 又因为极小左理想为单模, 所以它是一个不可约表示.

(2) 如果把 $\mathbb{C}G$ 和 $\mathrm{End}(L_i)$ 看作 $\mathbb{C}$ 上的向量空间, 则 λ_i 扩张为线性变换:

$$\begin{aligned}\tilde{\lambda_i} : \mathbb{C}G &\longrightarrow \mathrm{End}(L_i)\\ \sum_g c_g g &\longmapsto \sum_g c_g \lambda_i(g)\end{aligned}$$

我们证明 $\tilde{\lambda_i} : \mathbb{C}G \to \mathrm{End}(L_i)$ 确实是一个 $\mathbb{C}$-代数映射. 对任意的 $u_i \in L_i$ 和 $g, h \in G$ 有, $\tilde{\lambda_i}(gh) : u_i \mapsto (gh)u_i$, 而且 $\tilde{\lambda_i}(g)\tilde{\lambda_i}(h) : u_i \mapsto hu_i \mapsto g(hu_i)$. 根据结合性知 $(gh)u_i = g(hu_i)$. 从而 $\tilde{\lambda_i}(g)\tilde{\lambda_i}(h) = \tilde{\lambda_i}(gh)$. 注意到, 群代数存在如下单直和因子分解:

$$\mathbb{C}G = B_1 \oplus B_2 \oplus \cdots \oplus B_r$$

其中每个 B_i 不仅是 R 中的双边理想, 还几乎是 R 的子环 (幺元不同). 定义 $\mathbb{C}$-线性变换

$$\begin{aligned}F : \mathbb{C}G &\longrightarrow \mathbb{C}G\\ (b_1, b_2, \cdots, b_r) &\longmapsto (\tilde{\lambda_1}(b_1), \tilde{\lambda_2}(b_2), \cdots, \tilde{\lambda_r}(b_r))\end{aligned}$$

下证明 F 是 $\mathbb{C}$-代数映射. 为此, 只需证明其保持乘法. 现已证明只要 $b_i, b_i' \in B_i$, 就有:

$$F(b_i b_i') = \tilde{\lambda_i}(b_i b_i') = \tilde{\lambda_i}(b_i)\tilde{\lambda_i}(b_i') = F(b_i)F(b_i')$$

但若 $b_i \in B_i$ 和 $b_j \in B_j$, 其中 $i \neq j$, $b_j b_i = 0$, 这是因为每个 B 都是理想且 $\mathbb{C}G$ 是它们的直和. 另一方面, $F(b_i) \in B_i$ 和 $F(b_j) \in B_j$, 从而 $F(b_i)F(b_j) = 0$, 即 $F(b_i b_j) = 0$, 所以 F 是 $\mathbb{C}-$ 代数映射.

□

定义 6.5.12. G 是一个群, $\sigma, \tau : G \to \mathrm{GL}(n, \mathbb{C})$ 是两个复表示, 称 σ 和 τ **等价 (equivalent)**, 若存在非奇异 $n \times n$ 矩阵 P 满足, 对任意的 $g \in G$, $P\sigma(g)P^{-1} = \tau(g)$. 记 σ 与 τ 等价为 $\sigma \sim \tau$.

引理 6.5.13. *(1) 有限群 G 的每个不可约表示都与性质(6.5.11)给出的 λ_i 之一等价.*

(2) 有限 Abel 群的每个不可约表示都是线性的.

(3) 如果 $\sigma : G \to \mathrm{GL}(V)$ 是有限群 G 的表示, 则对每个 $g \in G$, $\sigma(g)$ 与一个对角矩阵相似.

证明. (1) 如果 $\sigma : G \to \mathrm{GL}(V)$ 是一个不可约表示, 则对应的 $\mathbb{C}G$-模 V^σ 是单模. 根据定理(6.3.8)知, 每个 $R-$ 单模 S 同构于某个 L_j. 于是, 存在某个 i, 使得 $V^\sigma \cong L_i$. 但 $L_i \cong V^{\lambda_i}$, 因此 $V^\sigma \cong V^{\lambda_i}$, 从而 $\tau \sim \lambda_i$.

(2) 因 G 是 Abel 群, $\mathbb{C}G = \sum_i B_i$ 是交换的. 因此一切 $n_i = 1$, 但 $n_i = \deg(\lambda_i)$.

(3) 若 $\sigma' = \sigma/\langle g\rangle$, 则 $\sigma'(g) = \sigma(g)$. 现在, σ' 是 Abel 群 $\langle g\rangle$ 的表示, 因此 (2) 蕴含模 $V^{\langle\sigma'\rangle}$ 是一维子模的直和. 如果 $V^{\langle\sigma'\rangle} = \langle v_1\rangle \oplus \langle v_2\rangle \oplus \cdots \oplus \langle v_m\rangle$, 则 $\sigma(g)$ 关于基 $v_1, v_2, \cdots, v_m$ 的矩阵是对角矩阵.

□

性质 6.5.14. *(1) 如果 $A = [a_{ij}]$ 和 $B = [b_{ij}]$ 是元素在交换环 R 中的 $n \times n$ 矩阵, 则迹满足性质:*

$$\mathrm{tr}(A + B) = \mathrm{tr}(A) + \mathrm{tr}(B)$$
$$\mathrm{tr}(AB) = \mathrm{tr}(BA)$$

(2) 如果 $B = PAP^{-1}$, 则 $\mathrm{tr}(B) = \mathrm{tr}(A)$.

证明. (1) 迹的加性知 $A + B$ 的对角线元素 $a_{ii} + b_{ii}$, 若用 $(AB)_{ii}$ 表示 AB 的第 i 行第 i 列元素, 则 $(AB)_{ii} = \sum_j a_{ij}b_{ji}$. 因此,

$$\mathrm{tr}(AB) = \sum_i (AB)_{ii} = \sum_{i,j} a_{ij}b_{ji} = \sum_{i,j} b_{ji}a_{ij} = \mathrm{tr}(BA)$$

(2)

$$\mathrm{tr}(B) = \mathrm{tr}((PA)P^{-1}) = \mathrm{tr}(P^{-1}(PA)) = \mathrm{tr}(A)$$

□

定义 6.5.15. 如果 $\sigma : G \to \mathrm{GL}(V)$ 是表示, 则它的特征标是指由迹函数定义的函数:

$$\chi_\sigma : G \to \mathbb{C}$$
$$g \mapsto \chi_\sigma(g) = \mathrm{tr}(\sigma(g))$$

称 χ_σ 为 σ **提供的特征标 (character afforded by σ)**. 一个不可约表示提供的特征标, 称为**不可约特征标 (irreducible character)**. 定义 χ_σ 的次数为表示 σ 的次数. 即 $\deg(\chi_\sigma) = \deg(\sigma) = \dim(V)$.

例 6.5.16. 特征标的一些例子.

(1) 由线性表示提供的特征标 θ 称为**线性特征标 (linear character)**, 即 $\theta = \chi_\sigma$. 其中 $\deg(\sigma) = 1$, 因每个线性表示都是不可约的, 所以每个线性特征标都是不可约的.

(2) 表示 $\lambda_i : G \to \mathrm{GL}(\lambda_i)$ 是不可约的, 则由 λ_i 提供的特征标:

$$\chi_i = \chi_{\lambda_i}$$

是不可约的.

(3) 由性质(6.5.11), 对每个 $u \in \mathbb{C}G$, $\chi_i(u)$ 是有意义的. 当然, 当 $j \neq i$ 时, 对一切 $u_j \in \mathrm{End}(L_j)$ 有 $\chi_i(u_j) = 0$, 从而:

$$\chi_i(u_j) = \begin{cases} \mathrm{tr}(\tilde{\lambda_i}(u_j)) & j = i \\ 0 & j \neq i \end{cases}$$

(4) 若 $\sigma : G \to \mathrm{GL}(V)$ 是任一表示, 则 $\chi_\sigma(1) = n$. 其中, n 是 σ 的次数. 这只需要注意到 $\sigma(1)$ 是单位矩阵, 它的迹是 $n = \dim(V)$.

(5) 设 $\sigma : G \to S_X$ 是群同态, 把 σ 看作是 $V = \langle X \rangle$ 上的表示. 对每个 $g \in G$, 矩阵 $\sigma(g)$ 是置换矩阵. 若 $\sigma(g)(x) = x$, 则 $\sigma(g)$ 第 x 行对角线元素为一, 否则为零. 于是:

$$\chi_\sigma(g) = \mathrm{tr}(\sigma(g)) = \mathrm{Fix}(\sigma(g))$$

$\mathrm{Fix}(\sigma(g))$ 是 g 的不动点个数. 换句话说, 若 X 是一个 $G-$ 集, 把每个 $g \in G$ 看作作用在 X 上, g 的作用的不动点的个数就是特征标的取值.

注 76. 特征标和表示的加法相容. 如果 $\sigma : G \to \mathrm{GL}(V)$ 和 $\tau : G \to \mathrm{GL}(W)$ 是两个复表示, 则 $\sigma + \tau : G \to \mathrm{GL}(V + W)$; 且满足:

$$\mathrm{tr}((\sigma + \tau)(g)) = \mathrm{tr}\left(\begin{bmatrix} \sigma(g) & 0 \\ o & \tau(g) \end{bmatrix}\right) = \mathrm{tr}(\sigma(g)) + \mathrm{tr}(\tau(g))$$

所以,

$$\chi_{\sigma+\tau} = \chi_\sigma + \chi_\tau$$

如果 σ 和 τ 是等价的, 则对一切 $g \in G$,

$$\mathrm{tr}(\sigma(g)) = \mathrm{tr}(P\sigma(g)P^{-1}) = \mathrm{tr}(\tau(g))$$

即它们有相同的特征标. 即 $\chi_\sigma = \chi_\tau$. 由此, 若 $\sigma : G \to \mathrm{GL}(V)$ 是一个表示, 则它的特征标 χ_σ 可以用 V 的一个合适的基来计算.

性质 6.5.17. *(1) 每个特征标 χ_σ 都可由 $\lambda_i : G \to \mathrm{GL}(L_i)$ 提供的不可约特征标 $\chi_i = \chi_{\lambda_i}$ 的 $\mathbb{N}$-线性组合表示. 即存在整数 $m_i \geq 0$, 使得:*

$$\chi_\sigma = \sum_i m_i \chi_i$$

(2) 等价表示有相同的特征标.

(3) G 的不可约表示特征标只有 $\chi_1, \chi_2, \cdots, \chi_r$.

证明. (1) 特征标 χ_σ 由 G 的表示 σ 产生, 而表示 σ 由 $\mathbb{C}G$-模 V 产生, 但 V 是半单模 (因为 $\mathbb{C}G$ 是半单环), 从而 V 是单模的直和 $V=\sum\limits_j S_j$. 根据定理(6.5.11), 如果 $R=\sum_j L_j$ 是左半单环, 其中 L_j 是极小左理想, 则每个单 $R-$ 模 S 同构于某个 L_j. 于是, 现存在某个极小左理想 L_i, 使得 $S_j\cong L_i$. 如果对于每个 i, $m_i\geq 0$ 是同构于 L_i 的 S_j 的个数, 则

$$\chi_\sigma=\sum_i m_i\chi_i$$

(2) 由命题 3 的 (2) 和推论 1 的 (1) 得到.

(3) 由 (2) 和推论 1 的 (1) 得到.

□

例 6.5.18. 对一切 $g\in G$, 具有 $\sigma(g)=1$ 的非平凡表示 $\sigma: G\to\mathbb{C}$ 所提供的线性特征标 χ, 称为**平凡特征标 (trivial representation)**. 于是, 对一切 $g\in G$, $\chi_1(g)=1$.

6.6 类函数

本次讨论班我们将介绍类函数的定义, 幂等元, 并介绍特征标与类函数之间的关系. 我们将看到, 有限群的两个表示等价当且仅当它们提供相同的特征标. 同时, 不可约特征标间存在一种关系. 最后我们将为全体类函数的集合配置一个内积, 并定义广义特征标.

定义 6.6.1. 一个函数 $\phi: G\to\mathbb{C}$ 称为**类函数 (class function)**, 如果它在共轭类上是常数. 即如果 $h=xgx^{-1}$, 则 $\phi(h)=\phi(g)$.

由表示 σ 提供的每个特征标 $\mathcal{X}_\sigma$ 都是一个类函数. 若 $h=xgx^{-1}$, 则:

$$\sigma(h)=\sigma(xgx^{-1})=\sigma(x)\sigma(g)\sigma(x)^{-1},$$

从而 $\mathrm{tr}(\sigma(h))=\mathrm{tr}(\sigma(g))$, 即 $\mathcal{X}_\sigma(h)=\mathcal{X}_\sigma(g)$. 反过来不成立, 不是每个类函数都是特征标. 例如, 若 $\mathcal{X}$ 是特征标, 则 $-\mathcal{X}$ 是一个类函数. 由于 $-\mathcal{X}(1)$ 是负数, 而维数不可能是负数, 故它不是特征标.

定义 6.6.2. 记一切类函数的集合 $\phi: G\to\mathbb{C}$ 为 $\mathrm{CF}(G)$:

$$\mathrm{CF}(G)=\{\phi: G\to\mathbb{C}: \text{对一切}x,g\in G,\phi(g)=\phi(xgx^{-1})\}.$$

注 77. 可以发现 $\mathrm{CF}(G)$ 是 $\mathbb{C}$ 上的向量空间. 一个元素 $u=\sum\limits_{g\in G}c_g g\in\mathbb{C}G$ 是复数的 n 元组, 即 u 是一个函数 $u: G\to\mathbb{C}$, 对一切 $g\in G$ 有 $u(g)=c_g$. 则可知 $\mathrm{CF}(G)$ 是 $\mathbb{C}G$ 的子环, 由于每一个类和都是一个类函数, 则有 $\mathrm{CF}(G)$ 是中心 $Z(\mathbb{C}G)$, 从而 $\dim(\mathrm{CF}(G))=r$, 其中 r 是 G 中共轭类的个数.

定义 6.6.3. 记 $\mathbb{C}G = B_1 \oplus \cdots \oplus B_r$, 其中 $B_i \cong \mathrm{End}(L_i)$, 并令 e_i 表示 B_i 的幺元; 因此:

$$1 = e_1 + \cdots + e_r,$$

其中 1 是 $\mathbb{C}G$ 的幺元, 元素 e_i 称为 $\mathbb{C}G$ 中的**幂等元 (idempotent)**.

易知

$$e_i e_j = \delta_{ij} e_i.$$

引理 6.6.4. *不可约特征标 $\mathcal{X}_1, \cdots, \mathcal{X}_r$ 形成 $\mathrm{CF}(G)$ 的基.*

证明. 由于 $\dim(\mathrm{CF}(G)) = r$, 则只需证明 $\mathcal{X}_1, \cdots, \mathcal{X}_r$ 是线性无关的. 由于对一切 $j \neq i$, $\mathcal{X}_i(u_j) = 0$; 特别地, $\mathcal{X}_i(e_j) = 0$. 另一方面, $\mathcal{X}_i(e_i) = n_i$, 其中 n_i 是 $\mathcal{X}_i$ 的次数, 这是因为 n_i 是 $n_i \times n_i$ 单位矩阵的迹. 若 $\sum\limits_i c_i \mathcal{X}_i = 0$, 则对一切 j 有:

$$0 = (\sum_i c_i \mathcal{X}_i)(e_j) = c_j \mathcal{X}_j(e_j) = c_j n_j.$$

于是, 对一切 $c_j = 0$. □

定理 6.6.5 (表示等价与特征标等价对应). *有限群 G 的两个表示等价, 当且仅当它们提供相同的特征标 $\mathcal{X}_\sigma = \mathcal{X}_\tau$.*

证明. 证明充分性, 由于每个表示都是完全可约的, 则存在非负整数 m_i 和 l_i 使得 $\sigma \sim \sum\limits_i m_i \lambda_i$ 和 $\tau \sim \sum\limits_i l_i \lambda_i$. 根据假设, 对应的特征标一致:

$$\sum_i m_i \mathcal{X}_i = \mathcal{X}_\sigma = \mathcal{X}_\tau = \sum_i l_i \mathcal{X}_i.$$

由于不可约特征标 $\mathcal{X}_1, \cdots, \mathcal{X}_r$ 是 $\mathrm{CF}(G)$ 的基, 所以对一切 i, $m_i = l_i$, 因此 $\sigma \sim \tau$. □

由于 $\mathcal{X}_i(1)$ 是 $n_i \times n_i$ 阶单位矩阵的迹, 则有:

$$n_i = \mathcal{X}_i(1) = \sum_j \mathcal{X}_i(e_j) = \mathcal{X}_i e_i,$$

其中 e_i 是 B_i 的幺元.

不可约特征标之间存在一种关系, 使得对它们的计算变得容易. 我们首先求幂等元 e_i 在 $\mathbb{C}G$ 的基 G 下的表达式. 易知, 对一切 $y \in G$, 有

$$\mathcal{X}_i(e_i y) = \mathcal{X}_i(y),$$

对于 $y = \sum\limits_j e_j y, e_j y \in B_j$, 则 $\mathcal{X}_i(y) = \sum\limits_j \mathcal{X}_i(e_j y) = \mathcal{X}_i(e_i y)$.

定理 6.6.6. 如果 $e_i = \sum\limits_{g\in G} a_{ig}g$, 其中 $a_g \in \mathbb{C}$, 则:

$$a_g = \frac{n_i\mathcal{X}_i(g^{-1})}{|\ G\ |}.$$

证明. 设 ψ 是正则特征标, 现在 $e_ig^{-1} = \sum\limits_h a_{ih}hg^{-1}$, 从而 $\psi(e_ig^{-1}) = \sum\limits_{h\in G} a_{ih}\psi(hg^{-1})$. 由于 $h = g$ 时 $\psi(1) =|\ G\ |$, 当 $h \neq g$ 时, $\psi(hg^{-1}) = 0$. 所以,

$$a_g = \frac{\psi(e_ig^{-1})}{|G|}.$$

另一方面, 由于 $\psi = \sum\limits_j n_j\mathcal{X}_j$, 则有:

$$\psi(e_ig^{-1}) = \sum_j n_j\mathcal{X}_j(e_ig^{-1}) = n_i\mathcal{X}_i(e_ig^{-1}),$$

由于 $\mathcal{X}_i(e_ig^{-1}) = \mathcal{X}_i(g^{-1})$, 所以 $a_{ig} = \frac{n_i\mathcal{X}_i(g^{-1})}{|G|}$.

□

现在可以给 $\mathrm{CF}(G)$ 配置一个内积.

定义 6.6.7. 如果 $\alpha, \beta \in \mathrm{CF}(G)$, 定义

$$(\alpha, \beta) = \frac{1}{|G|}\sum_{g\in G} \alpha(g)\overline{\beta(g)},$$

其中 $\bar{c}$ 表示复数 c 的复共轭.

易知我们定义了一个内积; 即对一切 $c_1, c_2 \in \mathbb{C}$:

(1) $(c_1\alpha_1 + c_2\alpha_2, \beta) = c_1(\alpha_1, \beta) + c_2(\alpha_2, \beta)$;

(2) $(\beta, \alpha) = \overline{(\alpha, \beta)}$.

定理 6.6.8 (不可约特征标的正交性). 不可约特征标 $\mathcal{X}_1, \cdots, \mathcal{X}_r$ 形成一个正交基; 即:

$$(\mathcal{X}_i, \mathcal{X}_j) = \delta_{ij}.$$

证明. 有:

$$e_j = \frac{1}{|G|}\sum_g n_j\mathcal{X}_j(g^{-1})g.$$

因此,

$$\begin{aligned}\mathcal{X}_i(e_j)/n_j &= \frac{1}{|G|}\sum_g \mathcal{X}_j(g^{-1})\mathcal{X}_i(g)\\ &= \frac{1}{|G|}\sum_g \mathcal{X}_i(g)\overline{\mathcal{X}_j(g)}\\ &= (\mathcal{X}_i, \mathcal{X}_j).\end{aligned}$$

由于 $\mathcal{X}_i(e_j)/n_j = \delta_{ij}$, 则得证. □

定义 6.6.9. 有限群 G 上的**广义特征标 (generalized character)**φ 是指线性组合:

$$\varphi = \sum_i m_i \mathcal{X}_i,$$

其中 $\mathcal{X}_1, \cdots, \mathcal{X}_r$ 是 G 的不可约特征标, 其中 $m_i \in \mathbb{Z}$.

定理 6.6.10 (不可约特征标的判定法则). *群 G 的一个广义特征标 θ 是不可约特征标当且仅当 $\theta(1) > 0$ 且内积满足 $(\theta, \theta) = 1$.*

6.7 特征标表和正交关系

本节我们将引入特征标表这个工具. 本节中我们利用特征标表的性质得到两组特征标表的两个正交关系, 并利用正交关系得到一些不可约特征标的性质, 利用特征标表工具重新证明了 Burnside 计数原理. 最后我们指出了对于有限群而言, 其复特征标表与共轭类, 正规子群的关系.

记号 1. *G 为有限群, 我们将其共轭类记为:*

$$C_1, C_2, \cdots, C_r,$$

在每个共轭类中选取一个代表元, 记为:

$$g_1, g_2, \cdots, g_r,$$

不可约特征标记为:

$$\chi_1, \chi_2, \cdots, \chi_r,$$

特征标的维数记为:

$$n_1 = \chi_1(1), n_2 = \chi_2(1), \cdots, n_r = \chi_r(1),$$

共轭类长度记为:

$$h_1 = \mid C_1 \mid, h_2 = \mid C_2 \mid, \cdots h_r = \mid C_r \mid .$$

定义 6.7.1. 群 G 的**特征标表 (character table)** 是指一个 $r \times r$ 的复矩阵:

$$A = (a_{ij})_{n \times n}$$

其中, $a_{ij} = \chi_i(g_j)$.

注 78. 我们经常令 $C_1 = 1$, 令 χ_1 为平凡特征标, 所以特征标表的第一行全是 1. 由例(6.5.16)可知, 第一列由特征标的维数组成, 即 $a_{i1} = \chi_i(1) = n_i$. 特征标表第 i 行由 $\chi_i(1), \chi_i(g_2), \cdots \chi_i(g_r)$ 组成. 因为其他的共轭类没有明显的排序方式, 所以一个有限群可以有多个特征标表. 注意到, $\mathrm{CF}(G)$ 的内积(6.6.7)是对共轭类中代表元 g_i 与 G 中所有元素 g 求和. 故此内积可以赋予某种特殊的" 权", 即:

$$(\chi_i, \chi_j) = \frac{1}{|G|} \sum_{k=1}^{r} h_k \chi_i(g_k) \overline{\chi_j(g_k)}$$

定理(6.6.8)说明了特征标表不同行的加权内积为 0, 与自身内积为 1.

例 6.7.2. (1) 一个特征标表可以有复元素. 例如, 表(1)给出的三阶循环群 $G = \langle x \rangle$ 的特征标表中 $\omega = e^{2\pi i/3}$ 是三次本原单位根.

$\mathbb{Z}_3$ 的特征标表 (1)

g_i	1	x	x^2
h_i	1	1	1
χ_1	1	1	1
χ_2	1	ω	ω^2
χ_3	1	ω^2	ω

(2) 将 Klein 群 $\mathbf{V}$ 用加法记号表示:

$$\mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\} = \{0, a, b, a+b\}.$$

可以将 $\mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$ 视为 $\mathbb{F}_2$ 上的线性空间, 并在其上定义在 $1, -1 \in \mathbb{C}$ 中取值的线性" 符号函数", 这些" 符号函数" 就是 Klein 群的不可约表示. 例如, 特征标 χ_2 可以由对 a 非平凡而对 b 平凡的函数得出:

$$\chi_2(v) = \begin{cases} -1 & v = 0;\ v = a+b \\ 1 & v = 0;\ v = b \end{cases}$$

表(2)给出了 V 的特征标表.

V 的特征标表 (2)

g_i	0	a	b	$a+b$
h_i	1	1	1	1
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

(3) 我们现在讨论特征标表(3), 三阶对称群 S_3 的特征标表. S_n 中两个置换是共轭的当且仅当二者有相同的轮换结构. 因此, S_3 有三个共轭类, 取其中代表元 $1, (12), (123)$. 在例(6.3.28)中, 我们知道此群有三个不可约表示: 平凡表示 λ_1, 符号表示 $\lambda_2 = sgn$ 以及一个三维表示表示 λ_3. 由于第二行是符号表示, 所以第二行利用 $1, (12)$ 是偶置换, (123) 奇置换 可以计算得到. 第三行有元素:

$$2 \ a \ b,$$

其中 a, b 可以通过特征标表的正交关系计算得到. 考虑第三行与前两行的加权内积:

$$2 + 3a + 2b = 0,$$

$$2 - 3a + 2b = 0.$$

解上述二元二次方程立得.

S_3 的特征标表 (3)

g_i	1	(12)	(123)
h_i	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

下述命题给出了特征标表列之间的内积.

引理 6.7.3. *如果 A 是有限群 G 的特征标表, 则 A 是非退化的, 而且其逆为 A^{-1} 的第 i 行第 j 列的元素为:*

$$\left(A^{-1}\right)_{ij} = \frac{h_i\overline{\chi_j(g_i)}}{\mid G \mid}.$$

证明. 如果 $B = (b_{ij})_{n\times n}$ 是如上所述的矩阵, 即 $b_{ij} = \frac{h_i\overline{\chi_j(g_i)}}{|G|}$. 则我们有:

$$(AB)_{ij} = \frac{1}{\mid G \mid}\sum_k \chi_i(g_k)h_k\overline{\chi_j(g_k)} = \frac{1}{\mid G \mid}\sum_g \chi_(g)\overline{\chi_j(g)} = (\chi_i, \chi_j) = \delta_{ij},$$

因为 $h_k\overline{\chi_j(g_k)} = \sum\limits_{y\in C_k}\overline{\chi_j(y)}$. 因此, $AB = I$. □

下面的结果是基础的.

定理 6.7.4 (特征标表的正交关系). *如果 G 是一个 n 阶有限群, 其共轭类为:*

$$C_1, \cdots, C_r$$

每个共轭类 C_i 的长度为 h_i, 代表元记为 g_i. 令 G 的不可约特征标为 $\chi_1, \cdots, \chi_r$, 且 $\chi_i(1) = \deg(\chi_i) = n_i$. 则我们有如下结论:

(1)

$$\sum_{k=1}^{r} h_k \chi(g_k)\overline{\chi_j(g_k)} = \begin{cases} 0 & , i \neq j \\ |G| & , i = j \end{cases}$$

(2)

$$\sum_{i=1}^{r} \chi(g_k)\overline{\chi_i(g_l)} = \begin{cases} 0 & , k \neq l \\ |G| & , j = l \end{cases}$$

证明. (1) 从定理(6.6.8)立得.

(2) 如果 A 是一个群 G 的特征标表, $B = \left[h_i\overline{\chi_j(g_i)}/ \mid G \mid\right]$, 我们在上一个定理中证明过 $AB = I$. 所以 $BA = I$, 那么 $(BA)_{kl} = \delta_{kl}$. 那么,

$$\frac{1}{|G|}\sum_i h_k\overline{\chi_i(g_k)}\chi_i(g_l) = \delta_{kl}.$$

□

第二正交关系说明了特征标表中不同两列的普通内积 (无加权但是取复共轭) 是零, 与自身内积是 $\mid G \mid /h_k$. 正交关系说明了下面的特殊情况.

推论 6.7.5. *(1)*

$$\mid G \mid = \sum_{i=1}^{r} n_i^2.$$

(2)

$$\sum_{i=1}^{r} n_i\chi_i(g_k) = 0, \text{其中} k > 1.$$

(3)

$$\sum_{k=1}^{r} h_k\chi_i(g_k) = 0, \text{其中} i > 1.$$

(4)

$$\sum_{k=1}^{r} h_k \mid \chi_i(g_k) \mid^2 = \mid G \mid .$$

证明. (1) 利用第一正交关系第一行与第一行的内积得到.

(2) 利用第二正交关系其他列与第一列的内积得到.

(3) 利用第一正交关系其他行与第一行的内积得到.

(4) 利用第一正交关系各行与自身内积得到.

□

我们现在用特征标表证明对群作用轨道计数的 Burnside 计数原理, 证明思路是首先把一个在集合 X 上的群作用写为一个线性表示的形式, 然后将群作用的不动点与这个空间的不变子空间联系起来并且给出与轨道数的联系, 然后构造一个特别的作用使得其迹就是这个空间的维数, 而且这与每个元素的不动点有关.

定理 6.7.6 (Burnside 计数原理). *如果 G 是一个有限群, X 是一个有限 $G-$ 集, N 是这个作用的轨道数, 那么:*

$$N = \frac{1}{\mid G \mid} \sum_{g \in G} \mathrm{Fix}(g),$$

其中 $\mathrm{Fix}(g)$ 是 g 的不动点个数.

证明. 令 V 是一个以 X 为基的复线性空间, 则 $G-$ 集可诱导出如下表示:

$$\begin{aligned} \sigma : G &\to \mathrm{GL}(V) \\ g &\mapsto \sigma(g) : x \mapsto g.x \end{aligned}$$

进一步, 如果 χ_σ 是由 σ 给出的特征标, 那么 $\chi_\sigma(g) = \mathrm{Fix}(g)$. 令 $\mathrm{O}_1, \cdots, \mathrm{O}_N$ 是 X 的轨道. 我们首先证明 $N = \dim(V^G)$, 其中 V^G 是不动点空间:

$$V^G = \{v \in V : \text{对任意} g \in G \text{有} gv = v\}.$$

对任意 i, 定义 s_i是所有O_i中x的和. 现证这些元素就是不动点空间的一组基. 这等价于证明这些元素线性独立而且张成了不动点空间. 任意 $u \in V^G$, 那么 $u = \sum\limits_{x \in X} c_x x$ 那么 $u = gu = \sum\limits_{x \in X} c_x gx$ 说明了 $c_{gx} = c_x$. 那么, 对任意 $x \in \mathcal{O}_j$, x 的系数和 gx 的系数是相同的, 也就是说同一个轨道中的元素系数是相同的. 于是, $u = \sum\limits_j c_j s_j$. 因此 $N = \dim(G)$. 现在定义如下线性映射:

$$\begin{aligned} T : V &\to V \\ v &\mapsto \frac{1}{\mid G \mid} \sum_{g \in G} \sigma(g)(v) \end{aligned}$$

首先映射 T 是个 $\mathbb{C}G-$ 代数映射, 且 $T \mid_{V^G} = Id$, 而且 $\mathrm{Im}(T) = V^G$, 这是因为对任意 $x \in X$, $x \notin V^G$, 这种元素必然存在, 否则群作用是平凡的, 从而定理得证. 但是对任意的 $u \in V$, 我们有 $\mathrm{Im}(T) \subseteq V^G$. 由于 $\mathbb{C}G$ 是半单的, 故存在直和补 W 使得, $V = V^G \oplus W$. 取 $w \in W$, 对任意的 $g \in G$, $\sigma(g)w \in W$, $T(w) \in W$, 所以 $T(w) \in \mathrm{Im}(T)$. 但是 $V^G \cap W = \{0\}$, 所以 $T|_W = 0$. 取 W 中基 $w_1, \cdots, w_l$ 及 $s_1, \cdots s_N, w_1, \cdots, w_l$ 是 V 的一组基, 那么:

$$\mathrm{tr}(T) = \frac{1}{\mid G \mid} \sum_{g \in G} \mathrm{tr}(\sigma(g)) = \frac{1}{\mid G \mid} \sum_{g \in G} \mathrm{Fix}(g).$$

而且:

$$\mathrm{tr}(T) = \dim(V^G).$$

这也就证明了:

$$N = \frac{1}{\mid G \mid} \sum_{g \in G} \mathrm{Fix}(g).$$

□

接下来用特征标表来寻找正规子群. 事实上, 我们可以看到, 正规子群就是由共轭类组成的子群.

定义 6.7.7. 如果 χ_τ 是由表示 $\tau : G \to \mathrm{GL}(V)$, 则

$$\mathrm{Ker}(\chi_\tau) = \mathrm{Ker}(\tau).$$

性质 6.7.8. 令 $\theta = \chi_\tau$ 是有限群 G 由表示 $\tau : G \to \mathrm{GL}(V)$ 给出的特征标.

(1) 对任意 $g \in G$, 有 $\mid \theta(g) \mid \leq \theta(1)$.

(2)

$$\mathrm{Ker}(\theta) = \{g \in G : \theta(g) = \theta(1)\}.$$

(3) 如果 $\theta = \sum\limits_j m_j \chi_j$, m_j 为正整数, 那么

$$\mathrm{Ker}(\theta) = \bigcap_j \mathrm{Ker}(\chi_j).$$

(4) 如果 N 是 G 的正规子群, 则有不可约特征标 $\chi_{i_1}, \cdots, \chi_{i_j}$, 使得:

$$N = \bigcap_{j=1}^{s} \mathrm{Ker}(\chi_{i_j})$$

证明. (1) 由 Langrange 定理, 对于任意的 $g \in G, g^{|G|} = 1$. 即 $\tau(g)$ 的特征值 $\epsilon_1 \cdots \epsilon_d$, $d = \theta(1)$ 是 $\mid G \mid$ 次单位根, 则 $\mid \epsilon_j \mid = 1$. 于是,

$$\mid \theta(g) \mid = \mid \sum_{j=1}^{d} \epsilon_j \mid \leq d = \theta(1).$$

(2) 如果 $g \in \mathrm{Ker}(\theta) = \mathrm{Ker}(\tau)$, 那么 $\tau(g) = I$. 且 $\theta(g) = \mathrm{tr}(I) = \theta(1)$. 反之, 如果 $\theta(g) = \theta(1) = d$, 则有 ϵ_j 全为 1 才满足, 即 $\tau(g) = I$, 且 $g \in \mathrm{Ker}(\tau)$.

(3) 对任意 $g \in G$, 有

$$\theta(g) = \sum_j m_j \chi_j(g);$$

特别的

$$\theta(1) = \sum_j m_j \chi_j(1).$$

由 (2), 如果 $g \in \mathrm{Ker}(\theta)$, 则 $\theta(g) = \theta(1)$. 但是如果 $g \notin \mathrm{Ker}(\chi_j)$, 即有 $\mid \chi_j(g) \mid < \chi_j(1)$. 于是 $\mid \theta(g) \mid < \theta(1)$, 矛盾. 反之, 如果 $g \in \chi_j$, 那么 $\chi_j(g) = \chi_j(1)$. 于是:

$$\theta(g) = \sum_j m_j \chi_j(g) = \sum_j m_j \chi_j(1) = \theta(1);$$

因此, $g \in \mathrm{Ker}(\theta)$.

(4) 相当于找到群 G 的一个表示下映射的核是 N. G/N 的正则表示 ρ 是忠实的, 其核为 $\{1\}$. 于是, 取 π 作为群 G 到 G/N 的自然映射, 我们得到一个以 N 为核的表示 $\rho\pi$. 如果 θ 是这个表示的特征标, 则必然有 $\theta = \sum\limits_j m_j \chi_j$, 其中 m_j 为正整数, 这是因为一个表示必然是不可约表示的直和. 由 (3), 结论得证.

□

例 6.7.9. (1) 由 S_4 特征标表可知, §4 只有 $\mathrm{Ker}(\chi_2) = A_4$ 和 $\mathrm{Ker}(\chi_3) = V$ 两个非平凡正规子群.

(2) 用正规子群是共轭类的并的视角可以得到 A_5 的单性. 我们知道 S_5 有五个共轭类, 长度分别为 $1, 12, 12, 15, 20$. 他们互相组合除了 $1, 60$ 外没有别的 60 的因子, 但是正规子群阶数必然是群的阶数的因子, 所以 A_5 没有非平凡正规子群.

6.8 诱导特征标

如何从一个小的子群的特征标构造大群的特征标是一个重要的问题. 如果小群的特征标易于计算, 那么知道小群的特征标后或许会对大群的特征标有所帮助. 我们先从正规子群入手. 正规子群是一个特殊的子群, 正规性使得商群成为可能. 对于有限群 G 的正规子群 H, 若有从商群 G/H 的表示:

$$\sigma : G/H \to \mathrm{GL}(V)$$

考虑自然映射 $\pi : G \to G/H$, 由此构造出一个新的表示:

$$\sigma\pi : G \to \mathrm{GL}(V)$$

表示本质上是群同态, 同态的复合自然还是同态. 注意到此时这个 G 上的表示是由 σ 诱导出来的. 具体而言, $\sigma\pi(g) = \sigma(gH)$, 从作用的角度看就是我们把群分成一系列的等价类 (陪集), 然后这些等价类中的作用都是一样的. 从群代数上的模的观点看, 我们有 $\mathbb{C}(G/H)$-模 V 诱导出了一个 $\mathbb{C}G$ 模 V. 随后我们有如下事实, 表示 $\sigma : G/H \to \mathrm{GL}(V)$ 不可约等价于 $\mathbb{C}(G/H) - V$ 模的不可约, 从而 $\mathbb{C}G$-模 V 不可约.

例 6.8.1. 作为一个例子, 我们下面讨论非交换 8 阶群 G 的表示. 因为 $|G| = 8 = 2^3$, 根据推论(5.1.17)知, G 必然有非平凡的中心, 即 $\mathrm{Z}(G) \neq \{1\}$. 其次, $|\mathrm{Z}(G)| \neq 4$, 否则我们有 $|G/\mathrm{Z}(G)| = 2$, 该商群为循环群, 此时不难证明 G 会被迫成为一个交换群, 与题设矛盾. 于是, $|\mathrm{Z}(G)| \neq 8$, 则只能有 $|\mathrm{Z}(G)| = 2$. 不妨记 $\mathrm{Z}(G) = \{1, z\}$. 下面考察 $G/\mathrm{Z}(G)$. 注意到 $G/\mathrm{Z}(G)$ 不会是同构于 $\mathbb{Z}_4$ 的循环群, 否则 G 为交换群. 而阶为 4 的群在同构意义下仅有 $\mathbb{Z}_4$及 $\mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$. 因此,

$$G/\mathrm{Z}(G) \cong \mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$$

$\mathbf{V}$ 用抽象的生成元形式可以表示成:

$$\mathbf{V} = \{1, a, b, ab\};\ \text{其中} a^2 = 1, b^2 = 1$$

下面, 我们计算 $\mathbf{V}$ 的特征标表: 考虑正则表示, 取复表示空间为 $\mathbb{C}\mathbf{V}$. 其中, 是 $\mathbb{C}\mathbf{V}$ 由 $\mathbf{V}$ 中的元素生成的 $\mathbb{C}-$ 线性空间. 其中, 维数 $\dim_{\mathbb{C}}(\mathbb{C}\mathbf{V}) = 4$. 注意到, 根据性质(6.7.5), 表示维数满足关系:

$$|\mathbf{V}| = 1 + (n_2)^2 + (n_3)^2 + (n_4)^2$$

容易得到 $n_2 = n_3 = n_4 = 1, r = 4$. 于是, $\mathbf{V}$ 有 4 个共轭类. 需要留意的是. 若是把 $\mathbf{V}$ 放在 S_4 的置换结构中, 则只有 2 个共轭类. 于是, 我们有分解:

$$\mathbb{C}\mathbf{V} \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$$

同时, $\mathbf{V}$ 是交换群, 其生成的 $\mathbb{C}$-线性空间, 作为群代数而言是交换的, 这也说明了这种分解的合理性. 另外, 根据主表示的例子(6.3.9)知, 元素 $\gamma = \sum\limits_{g \in G} g \in \mathbb{C}\mathbf{V}$ 生成的 $\mathbb{C}\mathbf{V}$ 模 $L_1 = \langle \gamma \rangle$ 是不可约的. 一个 $\mathbb{C}\mathbf{V}$ 不可约模对应了一个不可约的表示, 而这个不可约表示特征标就是 χ_1. 更具体地说, 存在群同态 $\lambda_1 : \mathbf{V} \to \mathrm{GL}(L_1) \cong \mathbb{C}^\times$, 且有 $\lambda(g)k\gamma = k\gamma$. 即正则表示 $\lambda(g) = 1$, 即对于任意的 $g \in \mathbf{V}$, $\chi_1(g) = 1$. 另外, 从 $\mathbb{C}\mathbf{V}$ 的分解看出, 其所有的极小左理想都同构于 $\mathbb{C}$. 于是, 其余的三个非平凡一维特征标由群同态 $\lambda_i : \mathbf{V} \to \mathrm{GL}(\mathbb{C}) = \mathbb{C}^\times$ 给出. 下面的计算将充分体现作为一维不可约表示的优势. 不难注意到, 对任意的 $a \in \mathbf{V}$, 我们由:

$$\chi_i(a^2) = \mathrm{tr}(\lambda(a^2)) = \mathrm{tr}([\lambda_i(a)]^2) = [\chi_i(a)]^2$$

如果对应的极小左理想作为 $\mathbb{C}$-线性空间的维数不是 1, 则 $\lambda_i(a)$ 导致一个矩阵, 进而 χ_i 括号中系数难以处理. 基于这个事实, 容易得到 $\chi_i(a) = \pm 1, \chi_i(b) = \pm 1$. 这 4 种情况将对应 4 种不可约特征标, 其中 $\chi_i(ab) = \chi_i(a)\chi_i(b)$. 这也是得益于一维特征标运算优势. 此时, 我们得到了 $\mathbf{V}$ 的特征标表, 如下表所示. 按照习惯, 记平凡的特征标记作 χ_1.

表 6.1: **V**的特征标表

g_i	1	a	b	ab
h_i	1	1	1	1
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

下面我们考察 G 的特征标表. 由已知的商群同态 $\lambda_i : G/\operatorname{Z}(G) \cong \mathbf{V} \to \mathrm{GL}(\mathbb{C})$, 不难得到 $G \xrightarrow{\pi} G/\operatorname{Z}(G) \cong V \xrightarrow{\lambda_i} \mathrm{GL}(\mathbb{C}) \cong \mathbb{C}^\times$. 作为一维表示, $\lambda_i\pi$ 构成 G 的 4 个不可约表示. 下面我们取表示空间为 $\mathbb{C}G$, 留意, 之前我们取 $\mathbb{C}\mathbf{V}$ 作为表示空间, 这里发生了改变. 利用关系(6.7.5):

$$|G| = 8 = 1 + (n_1)^2 + \cdots + (n_r)^2$$

事先, 我们不知道 r 的值, 但现在我们已经知道, 算平凡表示在内, 我们有至少 4 个不可约表示, 也就是上述关系可以为 $|G| = 8 = 1 + 1 + 1 + 1 + \cdots + (n_r)^2$. 于是, 只有唯一的可能性, $|G| = 8 = 1 + 1 + 1 + 1 + 2^2$. 于是, 我们有分解:

$$\mathbb{C}G \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C})$$

故第五个不可约特征标是一个二维不可约表示决定的特征标 χ_5. 维数为 2 的特征标的计算就不能用之前一维的表示的算特征标的技巧了, 但我们可以通过正交关系算出来. 我们设 G 的五个共轭类代表元为 $\{1, z, x, y, w\}$. 下面, 我们举例说明如何计算 $\chi_2(z)$. 为此, 我们考虑表示 $\lambda_2\pi(z) = \lambda_2(z\operatorname{Z}(G)) = \lambda_2(\operatorname{Z}(G)) = 1$, 其中 $\operatorname{Z}(G)$ 就是 $G/\operatorname{Z}(G) \cong \mathbf{V}$ 的单位元. 我们考察 $\mathbf{V}$ 的特征标表, 则有 $\chi_2(z) = 1$. 而对于 x, y, w, 可以不妨设 $x\operatorname{Z}(G)y\operatorname{Z}(G) = w\operatorname{Z}(G)$, 类似于上述计算可得特征标取值, 最后通过正交关系(6.7.4)可计算出二维的特征标 χ_5.

群 G 的特征标表

g_i	1	z	x	y	w
h_i	1	1	2	2	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	-2	0	0	0

倘使子群不是正规, 情况会变得复杂, 但我们仍然有方法从子群的表示构造大群的表示.

定义 6.8.2. H 为 G 的子群, 若有表示

$$\rho : H \to \mathrm{GL}(V)$$

这等价于我们在 V 上定义了一个 $\mathbb{C}H$-模结构. 于是, 我们可以在这基础上通过张量的办法实现纯量扩充, 得到一个 $\mathbb{C}G$-模, 从而给出一个 G 上的表示:

$$V\uparrow^G = \mathbb{C}G \otimes_{\mathbb{C}H} V$$

称通过上述方式得到的表示为**诱导表示 (induced representation)**. 注意到, 此时我们的表示空间作为集合仍然是 V, 但作为一个代数结构, 其上的标量乘法发生了变化, 使得更多的标量作用到 V 上是有意义的, 记这个新的代数结构为 V^G. 一个 $\mathbb{C}G$-模对应一个表示, 记此表示为:

$$\rho\uparrow^G : G \to V^G$$

诱导表示的特征标记作 $\chi_\rho\uparrow^G$

引理 6.8.3. *(1) 若 $H \subset G$, 则 $\mathbb{C}G$ 是一个由 $[G:H]$ 个生成元生成的自由的右 $\mathbb{C}H$-模.*
(2) 若该 $\mathbb{C}H$-模 V, 作为 $\mathbb{C}$ 线性空间有基 $\{e_1, e_2, \ldots, e_m\}$, 则 $\mathbb{C}G \otimes_{\mathbb{C}H} V$ 可以看作以 $\{t_1 \otimes e_1, t_1 \otimes e_2, \ldots, t_n \otimes e_m\}$ 为基的 $\mathbb{C}$-线性空间.

证明. (1) 子群对 G 的左陪集给出了群 G 的一个划分:

$$G = \bigcup_{i=1}^{n} t_i H$$

其中 $n = [G:H]$, 而 $M = \{t_1, t_2, \ldots, t_n\}$ 为 H 在 G 中的陪集代表元. 由此, 对任意的 $g \in G$, 必有某个 i 使得 $g \in t_i H$, 即存在 $h \in H$, 有 $g = t_i h$. 断言:$\{t_1, t_2, \ldots, t_n\}$ 构成右 $\mathbb{C}H$-模的一组基, 从而右 $\mathbb{C}H$-模为自由模. 任取 $u \in \mathbb{C}G$, $u = \sum\limits_{g\in G} a_g g$, 其中 $a_g \in \mathbb{C}$. 于是, $a_g g = a_g t_i h = t_i a_g h$. 而 $a_g h \in \mathbb{C}H$ 则 $u = \sum\limits_{g} t_i a_g h = \sum\limits_{i} t_i \eta_i$, 其中 $\eta_i \in \mathbb{C}H$ 是把各种项收集起来得到. 其次我们可以说明集合 M 是线性无关的. 为此, 考虑方程:

$$\sum_{i=1}^{n} t_i \eta_i = 0, \eta_i \in \mathbb{C}H$$

其中 η_i 形如 $\sum\limits_{h\in H} a_{ih} h$ 的形式. 将其带入上式有:

$$\sum_{i} a_{ih}(t_i h) = 0$$

其中 $t_ih \in G$. $\mathbb{C}G$ 作为 $\mathbb{C}$ 线性空间, 可知基 G 都是 $\mathbb{C}$-线性无关的, 从而 $t_ih = 0$. 但细心的读者会发现, 可能会有形如 $t_ih = t_jh'$, 但验算可知这是不可能的.

(2) $\mathbb{C}G = \bigoplus_i \langle t_i \rangle_{\mathbb{C}H} = \bigoplus_i t_i\mathbb{C}H$. $V = \bigoplus_j \mathbb{C}\langle e_j \rangle$. 对于 $\mathbb{C}G \otimes_{\mathbb{C}H} V$ 中的生成元 $u \otimes v$, 其中 $u \in \mathbb{C}G, v \in V$. 我们有:

$$u = \sum_{i=1}^{n} t_i\eta_i, v = \sum_{j=1}^{m} c_je_j, \text{其中} c_j \in \mathbb{C}, \eta_i \in \mathbb{C}H$$

于是有,

$$\begin{aligned} u \otimes v &= \left(\sum_{i=1}^{n} t_i\eta_i\right) \otimes \left(\sum_{j=1}^{m} c_je_j\right) \\ &= \sum_{j=1}^{m} c_j \left(\sum_{i=1}^{n} t_i\eta_i\right) \otimes e_j \\ &= \sum_{j=1}^{m} c_j \left(\sum_{i=1}^{n} t_i\right) \otimes (\eta_ie_j) \\ &= \sum_{i,j} c_j(t_i \otimes \eta_ie_j) \end{aligned} \tag{6.7}$$

对于上式的最后一步, 注意 V 上本来就有 $\mathbb{C}H$ 结构, 即存在表示 $\sigma : H \to \mathrm{GL}(V)$. 于是, 我们有 $\eta_ie_j = \sigma(\eta_i)e_j = \sum_{k=1}^{m} b_{jk}e_k$. 将其带入上式可得,

$$\begin{aligned} &= \sum_{i,j} c_j(t_i \otimes \eta_ie_j) \\ &= \sum_{i,j} c_j \left(t_i \otimes \sum_{k=1}^{m} b_{jk}e_k\right) \\ &= \sum_{i,j,k} c_jb_{jk}(t_i \otimes e_k) \end{aligned} \tag{6.8}$$

□

定理 6.8.4 (诱导特征标的计算公式). *若 χ_σ 是由表示 $\sigma : H \to \mathrm{GL}(V)$ 所提供的特征标, 其中 H 是 G 的子群, 则诱导特征标 $\chi_\sigma \uparrow^G$ 会有如下计算公式:*

$$\chi_\sigma \uparrow^G (g) = \frac{1}{|H|} \sum_{a \in G} \dot{\chi}_\sigma(a^{-1}ga)$$

其中,

$$\dot{\chi}_\sigma(x) = \begin{cases} 0 & , x \notin H \\ \chi_\sigma(x) & , x \in H \end{cases}$$

证明. 在引理(6.8.3)中, 我们已经证明了 $\mathbb{C}G \otimes_{\mathbb{C}H} V$ 是可以构成 $\mathbb{C}$ 线性空间, 以及如何找到他们的一组基. 诱导表示的表示空间就是这个线性空间. 计算诱导特征标, 只要找到 $\sigma\uparrow^G(g)$ 对应的矩阵就可以了. 由于 $g(t_i \otimes e_j) = (gt_i) \otimes e_j$, 其中对于 $gt_i \in G$, 必然有一个 $k(i)$, 使得 $gt_i = t_{k(i)}h_i, h_i \in \mathbb{C}H$. 于是, 我们有:

$$\begin{aligned} gt_i \otimes e_j &= t_{k(i)}h_i \otimes e_j \\ &= t_{k(i)} \otimes h_i e_j \\ &= t_{k(i)} \otimes \sigma(h_i)e_j \end{aligned} \tag{6.9}$$

而 $\sigma\uparrow^G(g)$ 作用到基 $\{t_1\otimes e_1, t_1\otimes e_2, \ldots, t_n\otimes e_m\}$ 上会产生一个 $nm\times nm$ 的矩阵. 事实上, 读者可以自行结合上式, 譬如把 $\sigma\uparrow^G(g)$ 作用到基 $\{t_1 \otimes e_1, t_1 \otimes e_2, \ldots, t_1 \otimes e_m\}$ 上, 可以发现作用后的像空间就是由 $\{t_{k(1)} \otimes e_1, t_{k(1)} \otimes e_2, \ldots, t_{k(1)} \otimes e_m\}$ 张成的. 稍微计算, 不难发现, 该 $nm \times nm$ 矩阵可以分成 $n \times m$ 的分块矩阵, 且其中有很多块是零矩阵. 计算特征标就是计算位于对角线上的矩阵块, 而小矩阵块位于对角线等价于 $k(i) = i$, 并且小矩阵块的迹就是 $\sigma(h_i)$ 的表示矩阵. 由此, 考虑:

$$\mathrm{tr}(\sigma\uparrow^G(g)) = \sum_{k(i)=i} \mathrm{tr}(\sigma(h_i))$$

而 $gt_i = t_{k(i)}h_i = t_ih_i$, 当且仅当 $h_i = t_i^{-1}gt_i \in H$, 也就是有:

$$\mathrm{tr}(\sigma\uparrow^G(g)) = \sum_{k(i)=i} \chi_\sigma(t_i^{-1}gt_i) = \sum_i \dot{\chi}_\sigma(t_i^{-1}gt_i)$$

其中, 上述式子 $t_i^{-1}gt_i \in H$ 才产生贡献. 此时, χ_σ 是 H 上的类函数, 但 t_i 未必落在 H 中, 故不可使用 χ_σ 作为类函数的性质. 因为 $t_i^{(}-1)gt_i \in H$, 故 $h^{-1}(t_i^{-1}gt_i)h \in H$, 于是 $(t_ih)^{-1}gt_ih \in H$. 此时, 我们有:

$$\sum_{h\in H} \dot{\chi_\sigma}(h^{-1}(t_i^{-1}gt_i)h) = |H| \sum_{h\in H} \dot{\chi}_\sigma(t_i^{-1}gt_i)$$

由此,

$$\begin{aligned} \chi_\sigma\uparrow^G(g) &= \sum_i \dot{\chi}\sigma(t_i{-}1gt_i) \\ &= \sum_i \frac{1}{|H|} \sum_{h\in H} \dot{(\chi)}_\sigma((t_ih)^{-1}gt_ih) \\ &= \frac{1}{|H|} \sum_{a\in G} \dot{\chi}_\sigma(a^{-1}ga) \end{aligned} \tag{6.10}$$

□

推论 6.8.5. 由上述公式(6.8.4), 不难推出有以下结论:

(1) $\chi_\sigma\uparrow^G(1)=\frac{1}{|H|}\sum\limits_{a\in G}\dot{\chi}_\sigma(a^{-1}a)=\frac{1}{|H|}\sum\limits_{a\in G}\dot{\chi}_\sigma(1)=\frac{|G|}{|H|}\chi_\sigma(1)=[G:H]\chi_\sigma(1)$.
(2) 若 $H\triangleleft G$, *则对任意的* $g\notin G$, $\chi\uparrow^G(g)=0$.

定理 6.8.6 (Frobuenius Reciprocity). *设* H *是群* G *的一个子群, 并设* χ *是* G *上的一个类函数,* θ *是* G *上的一个类函数, 则有:*

$$(\theta\uparrow^G,\chi)_G=(\theta,\chi\downarrow_H)_H$$

其中, $\chi\downarrow_H$ *表示把* χ *限制到* H *上. 而* $(*,*)_G$ *表示* $\mathrm{CF}(G)$ *上的内积,* $(*,*)_H$ *表示* $\mathrm{CF}(H)$ *上的内积.*

证明. 朴素的计算, 略去证明 □

用于计算诱导特征标的计算公式还可以有:

定理 6.8.7 (诱导特征标的计算公式). *设* H *是* G *的子群,* $\phi\in\mathrm{CF}(H),a\in G$, *若以* $\mathrm{C}(a)$ *表示* G *中包含* a *的共轭类, 则* $H\cap\mathrm{C}(a)$ *会被* H *中的共轭类划分. 设* $x_1,x_2,\ldots,x_m$ *为这些共轭类的代表元, 则有子群:*

$$\phi\uparrow^G(a)=|C_G(a)|\sum_{i=1}^{m}\frac{\phi(x_i)}{|C_H(x_i)|}$$

证明. 若 $H\cap\mathrm{C}(a)=\emptyset$, 则有 $\phi\uparrow^G(a)=0$. 故下面设 $H\cap\mathrm{C}(a)\neq\emptyset$. 因为, 对于某个 $t_0at_0^{-1}\in H$, 恰好有 $\mathrm{C}_G(a)$ 个 G 的元素, 使得 $tat^{-1}=t_0at_0^{-1}$. 于是根据定理(6.8.4)提供的计算公式, 有:

$$\begin{aligned}\phi\uparrow^G(a)&=\frac{1}{|H|}\sum_{t\in G}\dot{\phi}(tat^{-1})\\&=\frac{|\mathrm{C}_G(a)}{|H|}\sum_{y\in H\cap\mathrm{C}(a)}\phi(y)\end{aligned}\tag{6.11}$$

又对 $x_i\in H\cap\mathrm{C}(a)$, 恰有 $\frac{|H|}{|\mathrm{C}_H(x_i)|}$ 个于 x_i 在 H 中共轭的元素属于 $H\cap\mathrm{C}(a)$, 故上式可以变成:

$$\begin{aligned}\phi\uparrow^G(a)&=\frac{1}{|H|}\sum_{i=1}^{m}\frac{|H|}{|\mathrm{C}_H(x_i)|}\phi(x_i)\\&=|\mathrm{C}_G(a)|\sum_{i=1}^{m}\frac{\phi(x_i)}{|\mathrm{C}_H(x_i)|}\end{aligned}\tag{6.12}$$

□

6.9 代数整数

本节我们的任务是介绍代数整数. 回顾我们将复数 z 称为**代数数 (algebraic number)**, 如果其是非零多项式 $f(x) \in \mathbb{Q}[x]$ 的一个根. 因为 G 是一个有限群, Lagrange 定理告诉我们对于任意的 $g \in G$, 有 $g^{|G|} = 1$. 所以如果 $\sigma : G \to \mathrm{GL}(v)$ 是一个表示, 则对于所有的 g 都有 $\sigma(g)^{|G|} = I$; 因此, $\sigma(g)$ 的所有特征值都是 $|G|$ 次单位根, 进而都是代数整数. $\sigma(g)$ 的迹, 为特征值的和, 也为代数整数.

定义 6.9.1. 复数 α 称为**代数整数 (algebraic integer)**, 如果 α 为首一多项式 $f(x) \in \mathbb{Z}[x]$ 的一个根.

注 79. 注意定义中的首一是必须的. 每个代数数都是 $\mathbb{Q}[x]$ 中多项式的根, 去分母后可变为 $\mathbb{Z}[x]$ 中多项式的根. 显然每个普通的整数都是代数整数. 为了区分普通的整数与一般地代数整数, 我们称 $\mathbb{Z}$ 中元素为**有理整数 (rational integer)**.

下一性质说明, 代数整数的和与积都是代数整数.

性质 6.9.2. *设 $\alpha \in \mathbb{C}$ 并且定义 $\mathbb{Z}[\alpha] = \{g(\alpha) : g(x) \in \mathbb{Z}[x]\}$. 则*

(1) $\mathbb{Z}[\alpha]$ 为 $\mathbb{C}$ 的子环.

(2) α 为代数整数当且仅当 $\mathbb{Z}[\alpha]$ 是有限生成加性交换群.

(3) 所有代数整数的集合 $\mathbb{A}$ 是 $\mathbb{C}$ 的一个子环, 且 $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

证明. (1) 设 $g = 1$ 为常多项式, 则 $g \in \mathbb{Z}[x]$; 因此,$1 = g(\alpha)$, 所以 $1 \in \mathbb{Z}[\alpha]$. 设 $f(\alpha), g(\alpha) \in \mathbb{Z}[\alpha]$, 其中 $f(x), g(x) \in \mathbb{Z}[x]$. 现在 $f + g, fg$ 都在 $\mathbb{Z}[x]$ 中, 所以:

$$f(\alpha) + g(\alpha) \in \mathbb{Z}[\alpha]$$
$$f(\alpha)g(\alpha) \in \mathbb{Z}[\alpha]$$

因此, $\mathbb{Z}[\alpha]$ 为 $\mathbb{C}$ 的子环.

(2) 如果 α 是代数整数, 则存在首一多项式 $f(x) \in \mathbb{Z}[x]$ 以 α 为根. 我们证明如果 $\deg(f) = n$, 则 $\mathbb{Z}[\alpha] = G$, 其中 G 为所有线性组合 $m_0 + m_1\alpha + \cdots + m_{n-1}\alpha^{n-1}$ 的集合, $m_i \in \mathbb{Z}$. 显然, $G \subseteq \mathbb{Z}[\alpha]$. 对于反向的包含, 每个元素 $u \in \mathbb{Z}[\alpha]$ 有形式 $u = g(\alpha)$, 其中 $g(x) \in \mathbb{Z}[x]$. 因为 f 是首一的, 由带余除法给出 $q(x), r(x) \in \mathbb{Z}[x]$ 使得 $g = qf + r$, 其中或者 $r = 0$, 或者 $\deg(r) < \deg f = n$. 因此

$$u = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha) \in G.$$

因此, 加群 $\mathbb{Z}[\alpha]$ 是有限生成的. 相反地, 如果交换环 $\mathbb{Z}[\alpha]$ 的加群是有限生成的, 即作为交换群, $\mathbb{Z}[\alpha] = \langle g_1, \cdots, g_m \rangle$, 则每个 g_i 都是 α 幂的 $\mathbb{Z}-$ 线性组合, 其中 α 的最高次幂为 m. 因 $\mathbb{Z}[\alpha]$ 是一个交换环, 故 $\alpha^{m+1} \in \mathbb{Z}[\alpha]$. 因此, α^{m+1} 可表

示为 α 的低次幂的 $\mathbb{Z}-$ 线性组合. 即 $\alpha^{m+1}=\sum_{i=0}^{m} b_i\alpha^i$, 其中 $b_i\in\mathbb{Z}$. 因此, α 是 $f(x)=x^{m+1}-\sum_{i=0}^{m} b_ix^i$ 的根, 其为 $\mathbb{Z}[x]$ 中的首一多项式, 所以 α 是代数整数.

(3) 设 α,β 为代数整数; 令 α 为 n 次首一多项式 $f\in\mathbb{Z}[x]$ 的根, 令 β 为 m 次首一多项式 $g\in\mathbb{Z}[x]$ 的根. 现在 $\mathbb{Z}[\alpha\beta]$ 为 $G=\langle\alpha^i\beta^j : 0\le i<n, 0\le j<m\rangle$ 的加性子群. 因为 G 是有限生成的, 所以 $\mathbb{Z}[\alpha\beta]$ 也是有限生成的. (主理想整环上自由模的子模也是自由的) 故 $\alpha\beta$ 是代数整数. 类似的,$\mathbb{Z}[\alpha+\beta]$ 为 $\langle\alpha^i\beta^j : i+j\le n+m-2\rangle$ 的加性子群. 所以 $\alpha+\beta$ 也为代数整数. 对于代数整数如果不是整数, 那么就是无理数. 请读者自行证明.

□

定理 6.9.3 (群的复特征标取值是代数整数). *设 G 是有限群, 则对任意的特征标 χ 和任意的 $g\in G$, $\chi(g)$ 是代数整数.*

推论 6.9.4. *(i) 设 M 是一个有限生成交换群, 且对于某个环 R, 其作为左 $R-$ 模是忠实的, 则 R 的加性群也是有限生成的.*

(ii) 令 $\mathbb{Z}[\alpha]$ 为由复数 α 生成的 $\mathbb{C}$ 的子环. 如果存在一个忠实的 $\mathbb{Z}[\alpha]-$ 模其作为交换群是有限生成的, 则 α 是代数整数.

证明. (i) 因 M 是忠实的, 故环 R 同构于 $\mathrm{End}_{\mathbb{Z}}(M)$ 的子环. 因 M 是有限生成的, 所以 $\mathrm{End}_{\mathbb{Z}}(M)=\mathrm{Hom}_{\mathbb{Z}}(M,M)$ 也是有限生成的, 从而 R 也是有限生成的.

(ii) 由前面知识易得.

□

因为 $\mathbb{Z}[x]\subseteq\mathbb{Q}[x]$, 每个代数整数 α 都有唯一的最小多项式 $m(x)=\mathrm{Irr}(\alpha,\mathbb{Q})\in\mathbb{Q}[x]$, 且 m 在 $\mathbb{Q}[x]$ 中是不可约的.

推论 6.9.5. *如果 α 是代数整数, 则 $\mathrm{Irr}(\alpha,\mathbb{Q})$ 在 $\mathbb{Z}[x]$ 中.*

证明. 令 $p(x)\in\mathbb{Z}[x]$ 是以 α 为根的最小次数的首一多项式. 如果 $p(x)=G(x)H(x)$, 其中 $\deg(G)<p$, 且 $\deg(H)<\deg(p)$. 从而 α 是 G 或 H 的一个根. 由 Gauss 引理, 在 $\mathbb{Z}[x]$ 中存在因式分解 $p=gh$, 其中 $\deg(g)=\deg(G),\deg(h)=\deg(H)$. 事实上, 存在有理数 c,d 是得 $g=cG,h=dH$. 如果 a 是 g 的首项系数, b 为 h 的首项系数, 则 $ab=1$, 因为 p 是首一的. 因此, 我们可以假定 $a=1=b$, 由 $a,b\in\mathbb{Z}$; 即我们可以假定 g,h 都是首一的. 因为 α 为 g 或 h 的根, 这与 p 为以 α 为根的首一多项式矛盾. 而以 α 为根的唯一首一不可约多项式, 故 $p(x)=\mathrm{Irr}(\alpha,\mathbb{Q})$. □

注 80. 我们定义 α 的代数**共轭元 (conjugates)** 为 $\mathrm{Irr}(\alpha,\mathbb{Q})$ 的根. 我们定义 α 的**范数 (norm)** 为 α 所有共轭元的乘积的绝对值. 显然, α 的规范为 $\mathrm{Irr}(\alpha,\mathbb{Q})$ 的常数项, 所以它是整数.

现在我们可以证明如下结论.

定理 6.9.6. *有限群 G 的不可约特征标的次数 n_i 是 $|G|$ 的因子.*

证明. 由前面的知识我们知道, 如果 $\alpha=\frac{|G|}{n_i}$ 是代数整数, 那么它也是整数. 如果存在忠实 $\mathbb{Z}[\alpha]$-模 M 为有限生成 Abel 群, 则 α 为代数整数, 其中 $\mathbb{Z}[\alpha]$ 为 $\mathbb{C}$ 的包含 α 的最小子环. 所以我们有

$$e_i=\sum_{g\in G}\frac{n_i}{|G|}\chi_i(g^{-1})g=\sum_{g\in G}\frac{1}{\alpha}\chi_i(g^{-1})g.$$

因此, $\alpha e_i=\sum_{g\in G}\chi_i(g^{-1})g$. 但 e_i 是幂等的, 即 $e_i^2=e_i$, 所以

$$\alpha e_i=\sum_{g\in G}\chi_i(g^{-1})ge_i.$$

定义 M 为 $\mathbb{C}G$ 的由所有形式为 ξge_i 的元素生成的 Abel 子群, 其中 ξ 为 $|G|$ 次单位根, $g\in G$. 显然, M 为有限生成 Abel 群. 为了证明 M 是 $\mathbb{Z}[\alpha]$-模, 我们只需验证 $\alpha M\subseteq M$. 但注意到:

$$\alpha\xi ge_i=\xi g\alpha e_i=\xi g\sum_{h\in G}\chi_i(h^{-1})he_i=\sum_{h\in G}\chi_i(h^{-1})\xi ghe_i.$$

上式最后一项在 M 中, 因为 $\chi_i(h^{-1})$ 为 $|G|$ 次单位根的和. 最后, 如果 $\beta\in\mathbb{C}$ 且 $u\in\mathbb{C}G$, 则 $\beta u=0$ 当且仅当 $\beta=0$ 或 $u=0$. 因为 $\mathbb{Z}[\alpha]\subseteq\mathbb{C}$ 且 $M\subseteq\mathbb{C}G$, 这说明 M 是忠实的 $\mathbb{Z}[\alpha]$-模. □

引理 6.9.7. *如果 χ 是有限群 G 的特征标, $g\in G$, 则 $\chi(g)$ 为整数当且仅当 $\chi(g)$ 是有理数.*

证明. 因为 $\chi(g)$ 是代数整数, 由其性质即得. □

定义 6.9.8. 有限群 G 称为**共轭生成 (generator-conjugate)** 的, 如果对于任意的元素对 $g,g'\in G$ 满足 $\langle g\rangle=\langle g'\rangle$, 则它们是共轭的.

引理 6.9.9. *如果 G 是有限共轭生成群, 则对于任意的 $g\in G$ 和特征标 χ, 都有 $\chi(g)\in\mathbb{Q}$.*

注 81. 其逆命题也是正确的.

证明. 令 $\tau : G \to \mathrm{GL}(V)$ 为提供特征标 χ_τ 的表示. 如果 g 的阶为 m 且 ξ 为 m 次本原单位根, 则 $\tau(g)$ 的所有特征值为 ξ 的幂:

$$\chi_\tau(g) = \mathrm{tr}(\tau(g)) = \epsilon_1 + \cdots + \epsilon_t,$$

其中 $\epsilon_i = \xi^{j_i}$. 如果 g' 是 $\langle g \rangle$ 的另一生成元, 则 $g' = g^k$, 其中 $\gcd(k, m) = 1$. 因为 g' 阶为 m, $\tau(g')$ 的所有特征值也为 m 次单位根; 这些特征值为 ϵ_i^k: 如果 $\tau(g)(v) = \epsilon_i v$, 则 $\tau(g^k)(v) = \tau(g)^k(v) = \epsilon_i^k v$.

$$\chi_\tau(g') = \chi_\tau(g^k) = \mathrm{tr}(\tau(g^k)) = \epsilon_i^k + \cdots + \epsilon_t^k.$$

域扩张 $\mathbb{Q}(\xi)/\mathbb{Q}$ 为 Galois 扩张; 事实上, 其为 $x^m - 1$ 在 $\mathbb{Q}$ 上的分裂域. $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ 为循环群, 其生成元为 $\sigma_k : \xi \to \xi^k$, 其中 k 满足 $\gcd(k, m) = 1$. 现在,

$$\begin{aligned}\sigma_k(\chi_\tau(g)) &= \sigma_k(\epsilon_1 + \cdots + \epsilon_t) \\ &= \sigma_k(\epsilon_1) + \cdots + \sigma_k(\epsilon_t) \\ &= \epsilon_1^k + \cdots + \epsilon_t^k \\ &= \chi_\tau(g').\end{aligned}$$

由假设, g, g' 是共轭的, 所以 $\chi_\tau(g') = \chi_\tau(g)$, 因为 χ_τ 是类函数, 所以

$$\sigma_k(\chi_\tau(g)) = \chi_\tau(g).$$

因此 $\chi_\tau(g) \in \mathbb{Q}$, 由 σ_k 生成 $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$. □

定理 6.9.10. *如果 G 是有限共轭生成群, 则其特征标表中所有元素都是整数.*

注 82. 逆命题也是正确的.

推论 6.9.11. *S_n, D_8, $\mathbb{Q}$ 的特征标表中元素都是整数.*

6.10 Burnside 定理与 Frobenius 定理

有限群常表示的特征标理论在群论中有着重要的应用, 其中最具代表的是 Burnside 的 $p^m q^n$ 定理和 Frobenius 定理. 譬如, Thompson 因证明了"Frobenius 群的 Frobenius 核是幂零的" 获得 Fields 奖.

Burnside 的 $p^m q^n$ 和 Frobenius 定理的相关工作曾获得 Fields 奖. Burnside 的 $p^m q^n$ 定理给出了一大类有限可解群, 可解群与单群在群论中往往被视为" 对立的", 故 Burnside 的 $p^m q^n$ 定理被广泛应用于二十一世纪伟大的定理—有限单群的分类证明中.

Frobenius 定理主要阐述了 Frobenius 群的半直积 (semiproduct) 结构. 对于一般的群, 可以定义半直积 (semiproduct) 结构, 它是群上同调论 (cohomology of groups) 的基本语言.

有限群的复表示得益于 Molien 定理的简化, 如果有限群 G 的常表示中域 k 不为代数闭域, 则根据 Artin—Wedderburn 定理, 除环会存在群代数 kG 的直积表示中. 而对于除环, 我们已知的例子很少 (四元数代数, 一般线性代群, 单模的自同态环等). 除环的构造也并非容易. Brauer 在研究可除代数 (division algebra) 时, 引入了有限维中心单代数 (central simple algebra). 称有限维 k-代数 A 是**中心单代数**, 如果它作为环是单环且环的中心 $\mathrm{Z}(A) \cong k$. 对于有限维中心单代数引入相似等价关系 (similar equivalence) 可定义域 k 的 Brauer 群 $\mathrm{Br}(k)$. Brauer 群的重要之处在于, 域 k 的 Brauer 群 $\mathrm{Br}(k)$ 与域 k 上的有限维可除代数的所有同构类有一一对应的关系.

有限维代数的自同构群的计算非常困难, 它是代数数论中比较关心的问题. 得益于 Brauer 群, 自同构群的计算可以从 Brauer 群窥探. 利用群上同调的语言, Galois 扩张的 Galois 群与 Brauer 群有同构的关系. 因此, Brauer 群成为 Galois 表示的重要研究对象之一. 总而言之, 有限群常表示论的发展与 Galois 表示, 代数数论, 同调代数, 有限维代数表示, 代数拓扑, 代数几何, 复分析及 Lie 代数的表示等等其他数学分支有着非常紧密的联系.

6.10.1 群作用 (续)

为 Burnside 定理和 Frobenius 定理的证明做准备, 我们给出更多有关群作用的例子. G 是一个群, X 是一个集合. 记群 G 对集合 X 的群作用为 $G \curvearrowright X$. 给定群作用 $G \curvearrowright X$, 讨论集合 X 的轨道和群 G 的稳定子群及不动点是自然的.

例 6.10.1 (**对元素的共轭作用**). 当集合 $X = G$ 时, 考虑群对元素的共轭作用如下:

$$G \times G \longmapsto G$$

$$(g, a) \longmapsto g.a := gag^{-1}$$

此时, 对于任意的 $x \in G$, x 的轨道是 x 的共轭类; x 的稳定子群是 x 的中心化子.

$$O(x) = \{gxg^{-1} \mid g \in G\} = x^G$$

$$G_x = \{g \in G \mid gx = xg\} = C_G(x)$$

根据轨道—稳定子定理, 对 $x \in G$, x 的共轭类元素个数有下述关系:

$$\mid x^G \mid = \mid O(x) \mid = [G : G_x] = [G : C_G(x)]$$

因此, 有类方程:

$$|G| = |\operatorname{Z}(G)| + \sum_i |[G : C_G(x_i)]|$$

例 6.10.2 (对子群的共轭作用). 当集合 $X = \{H | H \leq G\}$ 时, 考虑共轭作用如下:

$$G \times X \longmapsto G$$

$$(g, H) \longmapsto g.H := gHg^{-1} = \{gag^{-1} \mid a \in H\}$$

注意到, 共轭子群彼此同构. 此时, 对于任意的 $H \in X$, H 的轨道是 H 的共轭子群; H 的稳定子群是 H 的正规化子.

$$O(H) = \{gHg^{-1} \mid g \in G\}(H \text{ 的共轭子群})$$

$$G_H = \{g \in G \mid gH = Hg\} = N_G(H)$$

根据轨道—稳定子定理, 对 $H \leq G$, H 的共轭子群个数有下述关系:

$$|\, O(H) \,| = [G : G_H] = [G : N_G(H)]$$

注意到, 子群 H 的中心化子 $C_G(H) \subseteq N_G(H)$. 根据 N—C 引理, 对于子群 H,

$$C_G(H) \lhd N_G(H)$$

且存在嵌入单同态:

$$\sigma : N_G(H)/C_G(H) \hookrightarrow \operatorname{Aut}(H)$$

同时, 对于 H 的内自同构群 $\operatorname{Inn}(H) \cong H/\operatorname{Z}(H)$, 且 $\operatorname{Inn}(H) \lhd \operatorname{Aut}(H)$. 可定义外自同构群:

$$\operatorname{Out}(H) = \operatorname{Aut}(H)/\operatorname{Inn}(H)$$

下面, 我们对群作用的传递性进行推广, 并且讨论一些重要的性质.

定义 6.10.3. G 是一个群, X 是集合, 称群作用 $G \curvearrowright X$ 是**传递的 (transitive)**, 如果 X 只有一个轨道. 更一般的, 称群作用 $G \curvearrowright X$ 是 $r-$ **传递的 (transitive)**, 如果对于 X 中的任意两个 r 维向量组 $(x_1, x_2, \cdots, x_r)$, $(y_1, y_2, \cdots, y_r)$, 存在 $g \in G$, 使得对于任意的 $1 \leq i \leq r$,

$$y_i = g.x_i$$

对于 $(x_1, x_2, \cdots, x_r)$ 的**稳定化子 (stabilizer)** 定义为:

$$G_{x_1, x_2, \cdots, x_r} = \{g \in G \mid \text{对于任意的 } 1 \leq i \leq r, g.x_i = x_i\} = \bigcap_{i=1}^{r} G_{x_i}$$

特别的, $r = 2$, 称群作用 $G \curvearrowright X$ 是**双传递的 (doubly transitive)**; $r = 3$, 称群作用 $G \curvearrowright X$ 是三**传递的 (triply transitive)**.

性质 6.10.4. *G 是一个有限群, X 是一个有限的 $G-$ 集. 对于任意的 $x \in X$, $X - \{x\}$ 是一个 G_x- 集.*

证明. 考虑自然继承的群作用, 对于任意的 $y \in X - \{x\}$, $y \neq x$; 对于任意的 $h \in G_x$, $h.y \neq x$, 于是 $h.y \in X - \{x\}$. 否则存在 $h \in G_x$, 使得 $h.y = x$. 于是

$$h.x = h.(h.y) = h^2.y = x$$

由归纳法, 对任意正整数 k, $h^k.y = x$. 因为 G 是有限群, 故 h 的阶是有限的, 记为 n. 当 $k = n$ 时, $x = (1.)y = y$, 矛盾. 故 $X - \{x\}$ 是一个 G_x 集. □

下面定理揭示了传递群作用和忠实群作用下, 群 G 的数量性质.

定理 6.10.5 (传递和忠实群作用下的数量性质). *G 是一个有限群, X 是传递 $G-$ 集. 集合 X 的基数 $\mid X \mid = n$, 对于任意的 $x \in X$, 成立以下数量性质:*

$$\mid G \mid = \mid X \mid \mid G_x \mid = n \mid G_x \mid$$

特别的, 当群作用还是忠实群作用时,

$$\mid G_x \mid \mid (n-1)!$$

证明. 因为 X 是传递的 $G-$ 集, 故 X 只有一个轨道. 即对任意的 $x \in X$, $O(x) = X$ 根据轨道—稳定子定理,

$$\frac{\mid G \mid}{\mid G_x \mid} = [G : G_x] = \mid O(x) \mid = \mid X \mid = n$$

从而, $\mid G \mid = n \mid G_x \mid$. 特别的, 当 X 是忠实的 $G-$ 集时, G 同构于 S_X 的子群. 根据性质(6.10.4), $X - \{x\}$ 是 G_x- 集, 且忠实. 因此, G_x 是 $S_{X-\{x\}}$ 的子群. 根据 Lagrange 定理,

$$\mid G_x \mid \mid (n-1)!$$

□

传递的群作用具有整体和局部的关系. 考察有限群 G 以及有限 $G-$ 集 X, 对任意 $x \in X$, $X - \{x\}$ 是 G_x- 集. 我们视此 G_x- 集是 $G-$ 集的" 局部信息". 下述定理阐述了传递群作用的整体和局部关系.

定理 6.10.6 (传递群作用的整体与局部关系). *G 是有限群, X 是有限 $G-$ 集. 如果 $r \geq 2$, 则 X 是 $r-$ 传递 $G-$ 集当且仅当, 对于任意的 $x \in X$, $X - \{x\}$ 是 $(r-1)-$ 传递的 G_x 集.*

证明. 充分性: 对于任意的 $x \in X$ 及 $(y_1, y_2, \cdots, y_{r-1})$, $(z_1, z_2, \cdots, z_{r-1})$ 是 $X - \{x\}$ 的 $(r-1)$ 维向量. 因为 X 是传递的 $G-$ 集, 存在 $g \in G$,

$$(x, z_1, z_2, \cdots, z_{r-1}) = g.(x, y_1, y_2, \cdots, y_{r-1}) = (g.x, g.y_1, g.y_2, \cdots, g.y_r)$$

注意到 $g.x = x$, 即存在 $g \in G_x$,

$$(z_1, z_2, \cdots, z_{r-1}) = (g.y_1, g.y_2, \cdots, g.y_{r-1}) = g.(y_1, y_2, \cdots, y_{r-1})$$

$X - \{x\}$ 是 $(r-1)-$ 传递 G_x 集.

必要性: 设 $(x_1, x_2, \cdots, x_r)$ 和 $(y_1, y_2, \cdots, y_r)$ 是 X 的 $r-$ 维向量组. 因为 $X - x_r$ 是 $(r-1)-$ 传递的 G_{x_r} 集, 于是存在 $g \in G_{x_r}$, 使得,

$$g.x_r = x_r$$

$$g.(x_1, x_2, \cdots, x_{r-1}) = (y_1, y_2, \cdots, y_{r-1})$$

同理, 存在 $h \in G_{y_1}$(取 $h = 1$ 即可), 使得,

$$h.y_1 = y_1$$

$$h.x_r = y_r$$

$$h.(y_2, y_3, \cdots, y_r) = (y_2, y_3, \cdots, y_r)$$

于是, 存在 $hg \in G$ 使得,

$$hg.(x_1, x_2, \cdots, x_r) = h.(y_1, y_2, \cdots, y_r) = (y_1, y_2, \cdots, y_r)$$

于是, X 是 $r-$ 传递的 $G-$ 集合. □

定理 6.10.7 ($r-$ **传递** $G-$ **集的数量关系**). *X 是含有 n 个元素的 $r-$ 传递 $G-$ 集合, 对于 X 中任意取定的 $r-$ 维向量组 $(x_1, x_2, \cdots, x_r)$, 则成立如下数量关系:*

$$| G | = n(n-1)\cdots(n-1+r) \mid G_{x_1, x_2, \cdots, x_r} \mid$$

特别的, 若 X 是忠实的 $G-$ 集, 则

$$| G_{x_1, x_2, \cdots, x_r} | \mid (n-r)!$$

证明. 采用数学归纳法. 当 $r = 1$ 时, 根据定理(6.10.5), 关系成立. 设 $r < k$, 等式成立, 则当 $r = k$ 时, G_{x_1} 是 $(r-1)$ 传递作用于 $X - \{x_1\}$. 利用定理(6.10.5), 关系成立. □

下面, 我们介绍一类特殊的 $r-$ 传递群作用, 它给出了一大类 Frobenius 群的例子.

定义 6.10.8. G 是一个有限群, 称 $r-$ 传递 G 集 X 是**严格传递 $G-$ 集 (sharply $r-$transitive)**, 如果 X 是 $r-$ 传递的, 且对于 X 中任意的 $r-$ 维向量组 $(x_1, x_2, \cdots, x_r)$, 其稳定化子

$$G_{x_1,x_2,\cdots,x_r} = \{1\}$$

注 83. 如果一个群作用既是传递群作用, 同时也是严格双传递群作用, 则此群作用是忠实的.

下面定理给出了严格 $r-$ 传递群作用的等价刻画.

定理 6.10.9. *G 是一个有限群, X 是含有 n 个元素的忠实且 $r-$ 传递的 $G-$ 集, 则以下等价:*

(1) X 是严格 $r-$ 传递 $G-$ 集.

(2) 对于 X 中的任意两个 $r-$ 维向量组 $(x_1, x_2, \cdots, x_r)$ 和 $(y_1, y_2, \cdots, y_r)$, 存在唯一的 $g \in G$, 使得,

$$(y_1, y_2, \cdots, y_r) = g.(x_1, x_2, \cdots, x_r)$$

(3) G 的阶有如下刻画:

$$\mid G \mid = n(n-1)\cdots(n-r+1)$$

(4) 对于 X 中的任意 r 个不同的元素, 只有 G 的乘法单位元 1 同时保持这 r 元素不动.

(5) 特别的, 当 $r \geq 2$ 时, 上述四条与下述命题等价: 对于任意的 $x \in X$, G_x- 集 $X - \{x\}$ 是严格 $(r-1)-$ 传递的.

证明. 在已有上述有关传递群作用的多个定理基础上, 此定理的证明是简单平凡的. 请自行推导验证. □

定义 6.10.10. G 是一个群, X 是集合, 称群作用 $G \curvearrowright X$ 是**忠实的 (faithful)**, 如果群作用诱导的群同态 $\sigma : G \longmapsto S_X$ 是单同态. 即

$$\mathrm{Ker}(\sigma) = \{g \in G \mid g.x = x, \text{对任意的} x \in X\} = \bigcap_{x \in X} G_x = \{1\}$$

称群作用是**正则的 (regular)**, 如果对于任意的 $x \in X$, 其稳定化子 $G_x = \{1\}$.

注 84. 群作用是正则的, 则一定是忠实的, 反之未必成立. 要说明群作用是忠实作用, 往往去说明群作用是正则的.

例 6.10.11 (左 (右) 平移作用). 当集合 $X = G$ 时, 考虑左平移作用如下:

$$G \times G \longmapsto G$$

$$(g,x)\longmapsto g.x:=gx$$

此时, 对于任意的 $a\in G$, a 的轨道是群 G; a 的稳定子群是平凡单位群 $\{1\}$. 也就是说, 左平移作用是传递的, 正则的, 故而也是忠实的. 这是因为, 任取 $b\in G$, $b=(ba^{-1})a=(ba^{-1}).a$. 左平移作用我们曾在证明 Cayley 定理时用到. 根据 Cayley 定理(5.1.1), 对于每一个群 G 都是 S_G 的子群, 从而可以诱导出正则表示, 这也是正则表示的由来.

$$G\xrightarrow{\delta}S_G\xrightarrow{\delta^*}\mathrm{GL}(kG)$$

$$g\longrightarrow\delta_g\longrightarrow\delta_g^*$$

例 6.10.12. H 是 G 的子群, 当集合 $X=G/H=\{gH\mid g\in G\}$ 是 G 关于 H 的陪集类时, 考虑陪集类的左平移作用如下:

$$G\times G/H\longmapsto G$$

$$(g,aH)\longmapsto g.aH:=gaH$$

此时, 对于任意的 $aH\in G/H$, aH 的轨道是 G/H; aH 的稳定子群是 H 关于代表元 a 的共轭子群.

$$O(aH)=G/H$$

$$G_{aH}=\{g\in G\mid gaH=aH\}=\{g\in G\mid a^{-1}ga\in H\}=\{g\in G\mid g\in aHa^{-1}\}=aHa^{-1}$$

同时, 如果对于任意的 $g\notin H$, 成立 $H\cap gHg^{-1}=\{1\}$, 则群作用是严格双传递的, 从而是忠实的. 这是因为, 对于任意的 $aH\neq bH$, $a^{-1}b\notin H$,

$$G_{aH}\cap G_{bH}=aHa^{-1}\cap bHb^{-1}=a(H\cap a^{-1}bH(a^{-1}b)^{-1})a^{-1}=\{1\}$$

例 6.10.13. $G=\mathrm{GL}(\mathbb{R}^n)\cong\mathrm{Mat}_n(\mathbb{R})$, $X=\mathbb{R}^n-\{0\}$. 考虑左平移作用如下:

$$G\times X\longmapsto G$$

$$(T,v)\longmapsto T.v:=T(v)$$

此时, 对于任意的 $v\in X$, v 的轨道是 X, 因而群作用是传递的; v 的稳定子群是 G 中以 v 为特征向量的含 1 为特征值的线性变换. 同时, 因为左平移是忠实的, 故 $G-$ 集 X 是忠实的.

$$O(v)=X$$

$$\begin{aligned}G_v&=\{T\in\mathrm{GL}(\mathbb{R}^n)\mid T(v)=v\}\\&=\{T\in\mathrm{GL}(\mathbb{R}^n)\mid T\text{是以 }v\text{ 为特征向量的含特征值为 1 的线性变换}\}\end{aligned}\tag{6.13}$$

例 6.10.14. k 是一个域, $f(x) \in k[x]$. $f(x)$ 不含重根. E/k 是 $f(x)$ 的分裂域. $G = \mathrm{Gal}(E/k) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_k = Id_k\}$, $X = \{a \in E \mid f(a) = 0\}$. 考虑群 G 对集合 X 的群作用:

$$G \times X \longmapsto G$$

$$(\sigma, x) \longmapsto \sigma.x := \sigma(x)$$

注意到, 根据引理(3.3.6)知, Galois 群 $\mathrm{Gal}(E/k)$ 对 $f(x)$ 根集 X 的群作用是忠实的. Galois 群 $\mathrm{Gal}(E/k)$ 对 $f(x)$ 根集 X 的群作用是传递的, 当且仅当 $f(x)$ 是域 k 上的不可约多项式. 如果 $f(x)$ 不可约, 则对于任意的 $\alpha, \beta \in X$, 存在同构:

$$\varphi : k(\alpha) \longmapsto k(\beta)$$

$$\sum_i a_i \alpha^i \longmapsto \sum_i a_i \beta^i$$

其中, $\varphi(\alpha) = \beta$. $\varphi|_k = Id_k$. 根据定理(3.3.47) , φ 可以延拓到 $f(x)$ 的分裂域 E/k 上. 即存在 $\Phi \in \mathrm{Aut}(E)$, 满足 $\Phi|_k = Id_k$, 即 $\Phi \in \mathrm{Gal}(E/k)$, 且 $\Phi(\alpha) = \varphi(\alpha) = \beta$, 于是 $\mathrm{Gal}(E/k)$ 对 $f(x)$ 根集 X 的作用是传递的. 反过来, 如果群作用是传递的, 假设 $f(x)$ 在域 k 上有不可约分解:

$$f(x) = p_1(x)p_2(x)\cdots p_t(x), \quad (t \geq 2)$$

设 $\alpha \in E$ 是 $p_1(x)$ 的根, $\beta \in E$ 是 $p_2(x)$ 的根; 因为 $f(x)$ 无重根, 所以 β 不是 $p_1(x)$ 的根. 群作用是传递的, 故存在 $\sigma \in \mathrm{Gal}(E/k)$, 使得 $\sigma(\alpha) = \beta$. 根据性质(3.3.4), Galois 群把不可约多项式的根映成不可约多项式的根. 于是 β 是 $p_1(x)$ 的根, 从而矛盾, 故 $t = 1$, 即 $f(x)$ 是不可约多项式.

注 85. 上述群作用, 对于一般的不可约多项式, 可以推出群作用是传递的. 群作用传递得出多项式不可约性只能针对无重根的多项式.

6.10.2 Burnside 定理

下面我们给出 Schur 引理的第二种形式, 它在各种表示论中都存在相应的形式, 起着十分重要的作用.

定理 6.10.15 (Schur 引理). *G 是一个有限群, $V/\mathbb{C}$ 是复数域 $\mathbb{C}$ 上的线性空间. 如果 $\sigma : G \mapsto \mathrm{GL}(V)$ 是一个不可约复表示, $\varphi \in \mathrm{End}_{\mathbb{C}}(V)$ 是线性变换, 且对任意的 $g \in G$ 满足:*

$$\varphi \circ \sigma(g) = \sigma(g) \circ \varphi$$

即对于任意的 $g \in G$, φ 与 $\sigma(g)$ 相似, 则 φ 是数乘线性变换, 存在复数 w, 使得:

$$\varphi = wId_v.$$

证明. 不可约复表示 σ 给出了一个 $\mathbb{C}G-$ 单模 V^σ: 对于任意的 $v \in V$,

$$g.v = \sigma(g)(v)$$

断言: 对于任意的 $g \in G$, 与 $\sigma(g)$ 相似的复线性变换 $\varphi \in \mathrm{End}_{\mathbb{C}}(V)$ 也是一个 $\mathbb{C}G$-模同态. 这是因为对于任意的 $v \in V$, 根据相似关系有:

$$\varphi(g.v) = \varphi \circ (\sigma(g)(v)) = \sigma(g) \circ \varphi(v) = g.\varphi(v)$$

根据 Schur 引理(6.3.6), $\mathrm{End}_{\mathbb{C}G}(V^\sigma)$ 是一个除环. 对于任意的 $w \in \mathbb{C}$, 由模自同态环的运算封闭性有 $\varphi - wId_V \in \mathrm{End}_{\mathbb{C}G}(V^\sigma)$. 复数域 $\mathbb{C}$ 是代数闭域, 故线性变换 φ 的特征值均在 $\mathbb{C}$ 中. 特别的, 当 w 为 φ 的特征值时, 存在 $0 \neq v \in V$, 使得

$$(\varphi - wId_V)(v) = 0$$

如果 $\varphi - wId_v \neq 0$, 则 $\varphi - wId_v$ 为 $\mathbb{C}G-$ 模同构, 自然也是复数域上的线性同构. 于是, $\det(\varphi - wId_v) \neq \{0\}$. 于是, $v = 0$, 矛盾. 故 $\varphi - wId_v = 0$. 即存在复数 w, 使得 $\varphi = wId_v$. 故 φ 是数乘变换. □

G 是一个有限群, 复群代数 $\mathbb{C}G$ 是半单的, B_i 为 $\mathbb{C}G$ 的单直和因子. 对于复群代数 $\mathbb{C}G$ 的每一个极小左理想 L_i, 存在不可约复表示

$$\lambda_i : G \longmapsto \mathrm{GL}(L_i)$$

$$g \longmapsto \lambda_i(g) : u_i \mapsto g.u_i$$

其中, $n_i = \deg(\lambda_i) = \dim_{\mathbb{C}}(L_i)$. 根据命题(6.5.11), 不可约复表示 λ_i 是正则表示在 L_i 的限制. 同时, λ_i 可以扩充为一个 $\mathbb{C}-$ 代数映射:

$$\tilde{\lambda_i} : \mathbb{C}G \longmapsto \mathrm{End}_{\mathbb{C}G}(\mathbb{C}G)$$

$$g \longmapsto \tilde{\lambda_i}(g) : \begin{cases} \tilde{\lambda_i}(g)(u_i) = \lambda_i(u_i) = g.u_i, & u_i \in B_i \\ \tilde{\lambda_i}(g)(u_j) = 0, & u_j \in B_j; j \neq i \end{cases}$$

即对于任意的 $g \in G$, 在极小左理想 L_i 下, $\tilde{\lambda_i}(g) = \lambda_i(g)$.

推论 6.10.16. *G 是一个有限群, L_i 是复群代数 $\mathbb{C}G$ 的极小左理想. λ_i 为 L_i 决定的不可约表示. $\tilde{\lambda_i}$ 为由 λ_i 诱导的 $\mathbb{C}-$ 代数映射, 则:*
(1) 对于任意 $z \in \mathrm{Z}(\mathbb{C}G)$, 存在 $w_i(z) \in \mathbb{C}$, 使得

$$\tilde{\lambda_i}(z) = w_i(z)I$$

(2) 函数

$$w_i : \mathrm{Z}(\mathbb{C}G) \longmapsto \mathbb{C}$$
$$z \longmapsto w_i(z)$$

是一个 $\mathbb{C}-$ 代数映射.

证明. (1) 由 Schur 引理第二形式(6.10.2), 令 $V = L_i$, $\sigma = \lambda_i$, $\varphi = \tilde{\lambda_i}(z)$, 因为在极小左理想 $V = L_i$ 下, $\tilde{\lambda_i}(g) = \lambda_i(g)$, 且 $\tilde{\lambda_i}$ 是 $\mathbb{C}-$ 代数映射, 则对于任意的 $g \in L_i$, $z \in \mathrm{Z}(\mathbb{C}G)$, Schur 引理的相似关系成立:

$$\tilde{\lambda_i}(z) \circ \lambda_i(g) = \tilde{\lambda_i}(z) \circ \tilde{\lambda_i}(g) = \tilde{\lambda_i}(z.g) = \tilde{\lambda_i}(g.z) = \tilde{\lambda_i}(g) \circ \tilde{\lambda_i}(z) = \lambda_i(g) \circ \tilde{\lambda_i}(z)$$

于是, 存在 $w_i(z) \in \mathbb{C}$, 使得: $\tilde{\lambda_i}(z) = w_i(z)I$.

(2) 因为 $\tilde{\lambda_i}$ 是 $\mathbb{C}-$ 代数映射, 容易验证 w_i 是一个 $\mathbb{C}-$ 代数映射.

□

下面, 我们利用不可约表示及其诱导的 $\mathbb{C}-$ 代数映射, 进一步研究群代数 $\mathbb{C}G$ 中心的性质.

性质 6.10.17. 设有限群 G 的共轭类为 $C_1, C_2, \cdots, C_r$, 每个共轭类的代表元为

$$g_1, g_2, \cdots, g_r$$

类和为 $z_1, z_2, \cdots, z_r$, 其中 $z_i = \sum_{g \in C_i} g$. 由引理(6.3.21), 类和 $z_1, z_2, \cdots, z_r$ 是 $\mathrm{Z}(\mathbb{C}G)$ 的一组基. 设 λ_i 为不可约表示, χ_i 为由 λ_i 决定的特征标, $w_i : \mathrm{Z}(\mathbb{C}G) \mapsto \mathbb{C}$ 是由不可约表示 λ_i 诱导的 $\mathbb{C}-$ 代数映射, 则以下有关群代数中心的性质成立:

(1) 对于任意的 i, j

$$w_i(z_j) = \frac{h_j \chi_i(g_j)}{n_i}$$

其中, h_j 为共轭类 C_j 的基数, $n_i = \deg(\lambda_i)$.

(2) 对于任意的 i, j 存在非负整数 a_{ijv}, 使得:

$$z_i z_j = \sum_v a_{ijv} z_v$$

(3) 对于任意的 i, j, $w_i(z_j)$ 是代数整数.

证明. 对于任意的 i, j, 对不可约表示 λ_i 及 $z_j \in \mathrm{Z}(\mathbb{C}G)$:

(1) 根据推论(6.10.16), 存在 $w_i(z_j) \in \mathbb{C}$, 使得 $\tilde{\lambda_i}(z) = w_i(z)I$, $\tilde{\lambda_i}$ 是诱导 $\mathbb{C}-$ 代数映射. 注意到:

$$\chi_i(z_j) = \mathrm{tr}(\tilde{\lambda_i})(z_j) = n_i w_i(z_j)$$

于是, 根据特征标是类函数有:

$$w_i(z_j)=\frac{\chi_i(z_j)}{n_i}=\frac{\chi_i\left(\sum\limits_{g\in C_j}g\right)}{n_i}=\frac{h_j\chi_i(g_j)}{n_i}$$

(2) 对于 $g_v\in C_v$, 根据群代数中乘法运算的定义, z_iz_j 中 g_v 的系数为下述有限集的基数, 记为 a_{ijv}^*:

$$\{(g_i,g_j)\in C_i\times C_j\mid g_ig_j=g_v\}$$

而 $z_v\in \mathrm{Z}(\mathbb{C}G)$ 的系数均相等. 令 $a_{ijv}=h_va_{ijv}^*$. 于是,

$$z_iz_j=\sum_v a_{ijv}z_v$$

(3) 令 $M=\langle w_i(z_j)\rangle\leqslant\mathbb{C}$ 是有限生成的 Abel 群. 因为 w_i 是 $\mathbb{C}-$ 代数映射, 故对于任意的 j,l, 根据 (2) 存在非负整数 a_{ijv}, 使得:

$$z_iz_j=\sum_v a_{ijv}z_v$$

$$w_i(z_j)w_i(z_l)=w_i(z_jz_l)=w_i\left(\sum_v a_{ijv}z_v\right)=\sum_v a_{ijv}w_i(z_v)\in M$$

即 M 对于复数的乘法运算封闭, 关于复数的乘法运算构成一个环. 从而, M 是一个有限生成 Abel 群上的 $\mathbb{Z}[w_i(z_j)]-$ 模 (模的数乘由环的乘法定义得到). 断言: M 是忠实的 $\mathbb{Z}[w_i(z_j)]-$ 模. 这是因为 $M\subseteq\mathbb{C}$, 如果存在 $m_1,m_2,\cdots,m_n$, 使得:

$$\left(\sum_{k=1}^{n}m_k(w_i(z_j))^k\right).M=0$$

由复数的乘法, 对任意的 $1\leq r\leq n$, $m_k=0$. 于是, 根据推论(6.9.4), $w_i(z_j)$ 是代数整数.

□

下面的一个性质阐述了某些特殊的不可约特征标在共轭类上的作用, 它是 Burnside 定理证明中有限群常表示特征标理论的重要体现.

性质 6.10.18. *G 是有限群, $C_1,C_2,\cdots,C_r$ 是 G 的共轭类, $z_1,z_2,\cdots,z_r$ 是类和. 设 $\mid C_i\mid=h_i$. $\chi_1,\chi_2,\cdots,\chi_r$ 是群 G 的不可约特征标, $n_i=\deg(\chi_i)$. 如果 $\gcd(n_i,h_j)=1$, 则要么 $\mid\chi_i(g_j)\mid=n_i$, 要么 $\chi_i(g_j)=0$.*

证明. 因为 $\gcd(n_i,h_j)=1$, 则存在 $s,t\in\mathbb{Z}$, 使得 $sn_i+th_j=1$.

(a) 对于任意的 $g_j \in C_j$, $n_i|\chi_i(g_j)$. 这是因为:

$$\frac{\chi_i(g_j)}{n_i} \cdot 1 = \frac{\chi_i(g_j)}{n_i} \cdot (sn_i + th_j) = s\chi_i(g_j) + \frac{th_j\chi_i(g_j)}{n_i} = s\chi_i(g_j) + tw_i(z_j)$$

根据性质(6.10.17), $w_i(z_j) = \frac{h_j\chi_i(g_j)}{n_i}$ 是代数整数. 代数整数的和仍为代数整数, 故 $\frac{\chi_i(g_j)}{n_i}$ 是代数整数.

(b) 当 $\chi_i(g_j) \neq 0$ 时, $\chi_i(g_j) = n_i$. 根据复特征标的有界性,

$$| \chi_i(g_j) | \leqslant \chi_i(1) = \deg(\chi_i) = n_i$$

故 $| \chi_i(g_j) | = n_i$.

(c) 当 $|\frac{\chi_i(g_j)}{n_i}| < 1$ 时, $\chi_i(g_j) = 0$. 记 $\alpha = \frac{\chi_i(g_j)}{n_i}$. 设 $m(x) \in \mathbb{Z}[x]$ 为 α 的极小多项式. 根据性质(6.9.5), $m(x)$ 在 $\mathbb{Q}[x]$ 是不可约多项式. 记 $m(x)$ 的常数项为 d. 设 $E/\mathbb{Q}$ 是多项式 $m(x)(x^{|G|}-1)$ 的分裂域. 设 α' 是 $m(x)$ 的另一个根. 因为 $m(x)$ 是不可约多项式, 故 Galois 群 $\mathrm{Gal}(E/\mathbb{Q})$ 对 $m(x)$ 的根集的群作用是传递的. 即存在 $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, $\alpha' = \sigma(\alpha)$. 因为有限群的特征标是单位根的和, 故

$$\alpha = \frac{1}{n_i}(\epsilon_1 + \epsilon_2 + \cdots + \epsilon_r)$$

其中 $\epsilon_1, \epsilon_2, \cdots, \epsilon_r$ 是 $|G|$ 次单位根. 从而,

$$\begin{aligned} \alpha' &= \sigma(\alpha) \\ &= \sigma\left(\frac{1}{n_i}(\epsilon_1 + \epsilon_2 + \cdots + \epsilon_r)\right) \\ &= \frac{1}{n_i}(\sigma(\epsilon 1) + \sigma(\epsilon_2) + \cdots + \sigma(\epsilon_r)) \end{aligned}$$

因为 $\mathrm{Gal}(E/\mathbb{Q})$ 把不可约多项式的根映成不可约多项式的根. 故:

$$\sigma(\epsilon)_1, \sigma(\epsilon)_2, \cdots, \sigma(\epsilon)_r$$

是 $|G|$ 次单位根. 于是 $|\alpha'| \leqslant 1$. 记 $\alpha_1, \alpha_2, \cdots, \alpha_k$ 是 $m(x)$ 的根, 考虑不可约多项式根 α 的范数 (不可约多项式根的模的乘积):

$$0 \leqslant N(\alpha) = d = \prod_{i=1}^{k} | \alpha_i | < 1$$

因为 $d \in \mathbb{Z}$, 故 $N(\alpha) = d = 0$, 当且仅当 $\alpha = 0$, 当且仅当 $\chi_i(g_j) = 0$.

□

在证明 Burnside 的 $p^m q^n$ 定理前, 我们先说明两个小性质, 方便在定理证明中使用.

性质 6.10.19. *G 是一个有限群, σ 为 G 的一个复表示. $\theta = \chi_\sigma$ 是由复表示 σ 诱导的特征标. 则对于 $\mathrm{Im}(\sigma) \cong G/\operatorname{Ker}(\theta)$ 的中心有如下关系:*

(1) 对于任意的 $g \in G$, $\mid \theta(g) \mid = \theta(1)$ 当且仅当, $\sigma(g)$ 为数量矩阵.

(2) 如果 σ 是不可约复表示, 则 θ 是不可约特征标, 则

$$\mathrm{Z}(G/\operatorname{Ker}(\theta)) = \{g\operatorname{Ker}(\theta) \mid g \in G :\mid \theta(g) \mid = \theta(1)\}$$

证明. (1) 对于任意的 $g \in G$,

$$\mid \operatorname{tr}(\sigma(g)) \mid = \mid \theta(g) \mid = \theta(1) = \operatorname{tr}(\sigma(1)) = n = \deg(\theta)$$

注意到 $\operatorname{tr}(\sigma(g))$ 是 n 次单位根的和, 设 $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ 是 n 次单位根. 因为

$$\mid \sum_{j=1}^{n} \epsilon_j \mid \leqslant \sum_{j=1}^{n} \mid \epsilon_j \mid = n$$

等号成立, 当且仅当 ϵ_j 均相等, 当且仅当 $\sigma(g)$ 是数量矩阵.

(2) 根据 (1), 对于任意的 $g \in G$, $\mid \theta(g) \mid = \theta(1)$ 当且仅当, $\sigma(g)$ 是数量矩阵, 当且仅当 $\sigma(g)$ 可与任意矩阵交换, 当且仅当 $g\operatorname{Ker}(\theta) \in G/\operatorname{Ker}(\theta)$.

□

在证明 Burnside 的 $p^m q^n$ 定理前, 我们回顾有限群不可约复特征标的正交关系及诱导关系.

性质 6.10.20. *G 是有限群, $C_1, C_2, \cdots, C_r$ 是 G 的共轭类, $g_1, g_2, \cdots, g_r$ 是每个共轭类的代表元. 设 $\mid C_i \mid = h_i$. $\chi_1, \chi_2, \cdots, \chi_r$ 是群 G 的不可约特征标, $n_i = \deg(\chi_i)$. 有限群的复特征标表是一个 n 阶复方阵:*

$$T = (\chi_i(g_j))_{ij}$$

满足如下正交关系及诱导关系:

(1) 对于第 i 个不可约特征标 χ_i 与第 j 个不可约复特征标 χ_j 满足正交关系:

$$(\chi_i, \chi_j) = \frac{1}{\mid G \mid} \sum_{k=1}^{r} h_k \chi_i(g_k) \overline{\chi_j(g_k)}$$

(2) 对于行关系, 遍历共轭类:

$$\sum_{k=1}^{r} h_k \chi_i(g_k) \overline{\chi_j(g_k)} = \begin{cases} 0, & i \neq j \\ \mid G \mid . & i = j \end{cases}$$

(3) 对于列关系, 遍历特征标*:*

$$\sum_{i=1}^{r}\chi_i(g_k)\overline{\chi_i(g_l)}=\begin{cases}0, & k\neq l\\ \frac{|G|}{h_k}. & k=l\end{cases}$$

(4) 群的数量关系*:* $|\,G\,|=\sum\limits_{i=1}^{r}n_i^2$*;* $n_i\,||\,G\,|$.

(5) 对于第 $k>1$ 列和, 以不可约特征标维数 n_i 为权重满足*:*

$$\sum_{i=1}^{r}n_i\chi_i(g_k)=0$$

(6) 对于第 $i>1$ 行和, 以共轭类基数 h_k 为权重满足*:*

$$\sum_{k=1}^{r}h_k\chi_i(g_k)=0$$

(7) 对于任意的第 i 行, 以共轭类基数 h_k 为权重满足*:*

$$\sum_{k=1}^{r}h_k\,|\,\chi_i(g_k)\,|^2=|\,G\,|$$

(8) 有限群不可约复表示特征标表是一个可逆矩阵, 且*:*

$$(A^{-1})_{ij}=\frac{h_i\overline{\chi_j(g_i)}}{|\,G\,|}$$

(9) 诱导特征标的计算*:* H 是有限群 G 的子群, $\sigma:H\mapsto \mathrm{GL}(V)$ 为子群 H 的一个复表示, 则

$$\chi_\sigma\uparrow^G(g)=\frac{1}{|\,H\,|}\sum_{a\in G}\dot{\chi}_\sigma(aga^{-1})$$

其中,

$$\dot{\chi}_\sigma(g)=\begin{cases}0, & g\notin H\\ \chi_\sigma(g), & g\in H\end{cases}$$

同时, $\chi_\sigma\uparrow^G(1)=[G:H]\chi_\sigma(1)$. 特别的, 如果 $H\lhd G$, 则对于任意的 $g\notin H$, $\chi_\sigma\uparrow^G(g)=0$.

(10) ***(Frobenius* 互反律*)****:* $H\leqslant G$ 是 G 的子群, χ 是 G 的类函数, θ 是 H 的复特征标, 则关于内积满足*:*

$$(\theta\uparrow^G,\chi)_G=(\theta,\chi\downarrow_H)_H$$

下面, 我们证明 Burnside 的 p^mq^n 定理.

定理 6.10.21 (Burnside 的 p^mq^n 定理).

(1) G 为有限非 Abel 单群, 则 $\{1\}$ 是群 G 唯一一个基数为素数幂的共轭类.

(2) 如果 "Burnside p^mq^n 定理" 对于有限群 G, $|G| = p^mq^n$, 其中 p, q 为素数, 则 "G 为可解群" 不成立, 则存在一个阶为 p^mq^n 的非 Abel 单群 G, G 有一个基数为素数幂的非平凡共轭类.

(3) "Burnside p^mq^n 定理" 成立: 对于有限群 G, $|G| = p^mq^n$, 其中 p, q 为素数, 则 G 为可解群.

证明. (1) 反证法.

G 为有限非 Abel 单群, 如果存在素数为 p, 使得有限群 G 有共轭类 C_j 基数满足: $|C_j| = h_j = p^e > 1$. 因为 G 是单群, 故对于群 G 的平凡不可约复特征标 χ_1, $\mathrm{Ker}(\chi_1) = G$; 对于群 G 的非平凡不可约复特征标 $\chi_i (i \geqslant 2)$, $\mathrm{Ker}(\chi_i) = \{1\}$. 根据性质(6.10.19),

$$\mathrm{Z}(G/\mathrm{Ker}(\chi_i)) = \{g\,\mathrm{Ker}(\chi_i) \mid g \in G : |\chi_i(g)| = \chi_i(1) = n_i\}$$

同时, 注意到 G 是非 Abel 单群, 故 $\mathrm{Z}(G) = \{1\}$. 所以

$$\mathrm{Z}(G/\mathrm{Ker}(\chi_i)) = \mathrm{Z}(G) = \{1\}$$

断言: 对于平凡不可约复特征标 χ_1, 对于 $g_j \in C_j$, $\chi_1(g_j) = 1$. 对于非平凡不可约复特征标 $\chi_i (i \geqslant 2)$:

(a) 如果 $\gcd(n_i, h_j) = 1$, 则 $\chi_i(g_j) = 0$. 根据性质(6.10.18): 要么 $|\chi_i(g_j)| = n_i$, 要么 $\chi_i(g_j) = 0$. 如果 $|\chi_i(g_j)| = n_i$, 则

$$g_j = g_j\,\mathrm{ker}(\chi_i) \in \mathrm{Z}(G/\mathrm{Ker}(\chi_i)) = \{1\}$$

于是 $C_j = \{1\}$, 矛盾. 故 $\chi_i(g_j) = 0$.

(b) 如果 $\gcd(n_i, h_j) \neq 1$, 则 $p \mid n_i$. 从而存在 $\alpha_i \in \mathbb{Z}$, 使得 $n_i = p\alpha_i$.

根据有限群复表示特征表标的正交关系: 对于第 $j > 1$ 列:

$$\sum_{i=1}^{r} n_i\chi_i(g_j) = 0$$

其中, $n_i = \chi_i(g_j)$; 特别的 $n_1 = \chi_i(g_j) = 1$. 令 $\beta = \sum_{i=1}^{t} \alpha_i$, 根据上述分析所得到的 $\chi_i(g_j)$ 的取值情况, 我们有:

$$0 = \sum_{i=1}^{r} n_i\chi_i(g_j) = 1 + p\beta$$

从而,

$$\beta = -\frac{1}{p}$$

因为 β 是代数整数, 故 $p = \pm 1$. 矛盾.

(2) 如果 Burnside 的 $p^m q^n$ 定理不成立, 则以下集合 X 非空:

$$X = \{G\text{是不可解群} \mid \text{存在素数 } p, q \text{ 及正整数 } m, n \text{ 使得}, \mid G \mid = p^m q^n\}$$

选取集合 X 中阶数最小的群为 G, G 是不可解群, 且存在素数 p, q 及正整数 m, n 使得 $\mid G \mid = p^m q^n$. 因为 G 是不可解群, 故 G 是非 Abel 群. 下面, 我们分两种情况进行讨论:

(A) G 不是单群, 即存在非平凡的正规子群 H, 则根据性质(3.3.21), 可解群的子群与商群均是可解群, 故 H 及 G/H 是可解群. 又由 Lagrange 定理, $H \in X$, $G/H \in X$, 这与 G 的选取矛盾.

(B) G 是单群, 则 G 没有非平凡的正规子群. 设 Q 为 G 的 Sylow-q 子群.

(a) 如果 $Q = \{1\}$, 则 G 是一个 $p-$ 群, 根据 $p-$ 群性质(5.1.17), G 有非平凡中心, 从而 G 不是单群. 矛盾. 事实上, 根据 $p-$ 群性质, 有限 $p-$ 群均是可解群, 这也与 G 的选取矛盾.

(b) 如果 $Q \neq \{1\}$, 则 Q 也是一个 $q-$ 群, $\mathrm{Z}(Q) \neq \{1\}$. 即存在 $1 \neq x \in \mathrm{Z}(Q)$, 注意到 $Q \subseteq C_G(x)$, 从而有如下等式:

$$p^m = [G : Q] = [G : C_G(x)][C_G(x); Q]$$

于是 $[G : C_G(x)] \mid p^m$, 根据元素上的群作用(6.10.1),

$$\mid x^G \mid = [G : C_G(x)] = p^k$$

其中 $k \geqslant 1$.

从而存在一个阶为 $p^m q^n$ 的非 Abel 单群 G, G 有一个基数为素数幂的非平凡共轭类.

(3) 由 (1), (2) 立即得出, 对于有限非 Abel 单群, $\{1\}$ 是群 G 唯一一个基数为素数幂的共轭类. 矛盾.

□

6.10.3 Frobenius 定理

有限群常表示特征标理论的另一个早期应用是 Frobenius 定理的证明.

记号 2. *G 是一个群, 记*

$$G^\sharp = \{g \in G \mid g \neq 1\}$$

如果 X 是一个 $G-$ 集, 对于任意的 $x, y \in X$, 记

$$G_{x,y} = \{g \in G \mid g.x = x且g.y = y\} = G_x \cap G_y$$

下面, 我们来定义 Frobenius 群.

定义 6.10.22. G 是一个有限群, 称 G 是一个 **Frobenius 群**, 如果存在传递的 $G-$ 集 X, 使得 G 满足如下性质:

(1) 对于任意的 $g \in G^\sharp$, g 至多有一个不动点.

(2) 存在 $g \in G^\sharp$, g 恰有一个不动点.

此时, 对于 $x \in X$, 称群 G 关于 x 的稳定化子 G_x 为 Frobenius 群 G 的 **Frobenius 补 (complement)**.

注 86. 我们对于 Frobenius 群给出一些注记:

(A) 下面进一步对 Frobenius 群定义中的两条进行阐述. $G-$ 集 X 是传递的, 则:

(a) 定义中的条件 (1), 等价于 $G-$ 集 X 是严格双传递的. 即对于任意的 $g \in G^\sharp$, g 至多有一个不动点, 当且仅当对于任意的 $x, y \in X$, $G_{x,y} = \{1\}$.

(b) 定义中的条件 (2), 等价于存在 $x \in X$, $G_x \neq \{1\}$.

(c) 根据定义中的条件 (1), 群作用诱导的群同态 $\sigma : G \mapsto S_x$ 是单同态. 因为,

$$\mathrm{Ker}(\sigma) = \bigcap_{x \in X} G_x$$

从而群作用是忠实的. 但因为条件 (2), 群作用不是正则的.

(d) 对任意的 $g \in G^\sharp$, g 不含不动点当且仅当, 对任意的 $x \in X$, $G_x = \{1\}$ 当且仅当, $G-$ 集 X 是正则的.

(B) G 是一个有限群, X 是有限传递的 $G-$ 集. 如果对于任意的 $g \in G^\sharp$, g 不含不动点 (即 X 是一个正则的 $G-$ 集), 则称 $G-$ 集 X 是**无不动点的 (fixed—point—free)**. Thompson 证明了: 如果有限群 H 存在无不动点的素数阶自同构 (fixed—point—free automorphism), 则 H 为幂零群. 其中, 有限群 H 存在无不动点的素数阶自同构指: 存在素数 p 及 $\alpha \in \mathrm{Aut}(H)$, 使得 $\alpha^p = Id_H$. 则考虑 α 生成的素数阶循环群 $G = \langle \alpha \rangle$ 对有限群 H 的群作用:

$$G \times H \longmapsto H$$

$$(\alpha^k, h) \longmapsto \alpha^k.h := \alpha^k(h)$$

如果有限群 H 在上述群作用是无不动点的, 则 H 是幂零群. 而 Frobenius 群是有不动点的一类有限群, 在某种意义上是幂零群 “对立”.

(C) 通过标准的证明方式去证明一般形式的定理是群论, 乃至数学中常见的特点. 对于群论中定理证明而言, 我们首先通过对群做一些额外的限制, 使得它满足更多的性质, 从某种特殊情形出发; 然后再逐渐放宽对群的限制, 考察更加一般 (困难) 的情形. 这种证明的策略经常会令群满足某些并不自然的条件或假设 (这些条件是人为加以限制的), 而这些条件和假设一旦在其它情况谈及, 数学工作者为方便达成共识, 会对这些性质或条件给出标准的定义. 因此, 群论中有些定义看起来是不甚自然的, 例如 Frobenius 群, 某种意义上是幂零群研究过程中的产物.

下面我们给出一类 Frobenius 群的例子.

例 6.10.23.

(1) 三阶置换群 S_3 是 Frobenius 群. 设集合 $X = \{1, 2, 3\}$. X 是传递的 S_3 集. 同时, X 是忠实的 S_3 集, 因为对任意的 $\alpha \in S_3^\sharp$, 置换 α 至多保持一个元素不动. (Frobenius 群的条件 (1)). 同时, 存在 $\langle (i,j)(k) \rangle \in S_3^\sharp (1 \leqslant i, j, k \leqslant 3)$ 恰有一个不动点 (Frobenius 群的条件 (2)). 因为, 群作用传递且严格双传递知, 群作用是忠实的.

(2) 事实上, 如果 $|\ X\ | \geqslant 3$, $G-$ 集 X 是非正则的严格双传递, 则有限群 G 一定是 Frobenius 群.

下面定理给出了 Frobenius 群的抽象判别准则, 它表明一个有限群是否为 Frobenius 群不依赖于外界的集合, 只由自身的结构和性质决定.

定理 6.10.24 (Frobenius 群的抽象判别准则). *一个有限群 G 为 Frobenius 群当且仅当, G 中存在一个非平凡的子群 H, 使得对于任意的 $g \notin H$, $H \cap gHg^{-1} = \{1\}$.*

证明. 充分性: 若 G 为 Frobenius 群, 令 X 为传递的 $G-$ 集, 使得存在 $x \in X$, $G_x \neq \{1\}$. 令 $H = G_x \leqslant G$. 于是, 对于任意的 $g \notin H = G_x$, 令 $y = g.x \neq x$. 因为同一轨道不同元素的稳定化子彼此共轭, 于是

$$gHg^{-1} = gG_xg^{-1} = G_{gx} = G_y$$

因为 Frobenius 群是严格双传递的, 故

$$H \cap gHg^{-1} = G_x \cap G_{gx} = G_{x,g.x} = G_{x,y} = \{1\}$$

必要性: 如果有限群 G 存在非平凡的子群 H, 满足对任意 $g \notin H$, $H \cap gHg^{-1}$. 令 $X = G/H$ 为 H 在 G 中的左陪集. 考虑左陪集上的左平移作用:

$$G \times G/H \longmapsto G$$

$$(g, aH) \longmapsto g.aH := gaH$$

此时, 对于任意的 $aH \in G/H$, aH 的轨道是 G/H; aH 的稳定子群是 H 关于代表元 a 的共轭子群.

$$O(aH) = G/H$$

$$G_{aH} = aHa^{-1}$$

同时, 如果对于任意的 $g \notin H$, 成立 $H \cap gHg^{-1} = \{1\}$, 则群作用是严格双传递的, 从而是忠实的. 这是因为, 对于任意的 $aH \neq bH$, $a^{-1}b \notin H$,

$$G_{aH} \cap G_{bH} = aHa^{-1} \cap bHb^{-1} = a(H \cap a^{-1}bH(a^{-1}b)^{-1})a^{-1} = \{1\}$$

又因为 $H \neq \{1\}$, 所以 $G_{aH} = aHa^{-1} \neq \{1\}$. 于是, 有限群 G 是 Frobenius 群. □

为进一步阐述 Frobenius 群的结构, 我们引入 Frobeniu 核. 对于一般的有限群及相应的群作用, 我们也可以定义 Frobenius 核.

定义 6.10.25. G 是一个群, X 是一个 $G-$ 集, 定义群 G 的 **Frobenius 核 (kernel)** 如下:

$$N = \{1\} \cup \{g \in G \mid g\text{没有不动点}\}$$

注 87. 特别的, 对于传递的 $G-$ 集 X 而言, Frobenius 核 N 可以用 G 的稳定子群来刻画:

(1) 对于传递的 $G-$ 集 X 而言, 任选 $x \in X$ 为轨道代表元. Frobenius 核 N 具有如下形式:

$$N = \{1\} \bigcup \left(G - \bigcup_{g \in G} gG_x g^{-1} \right)$$

这只需要注意到,

$$\begin{aligned}
(N^\sharp)^c &= \{a \in G \mid \exists y \in X, a.y = y\} \\
&= \{a \in G \mid \exists g \in G, a.(g.x) = g.x\} \\
&= \{a \in G \mid \exists g \in G, (g^{-1}ag).x = x\} \\
&= \{a \in G \mid \exists g \in G, g^{-1}ag \in G_x\} \\
&= \{a \in G \mid \exists g \in G, a \in gG_x g^{-1}\} \\
&= \bigcup_{g \in G} gG_x g^{-1}
\end{aligned}$$

于是,

$$N^\sharp = \left(G - \bigcup_{g \in G} gG_x g^{-1} \right)$$

(2) 对于传递的 $G-$ 集 X 而言, Frobenius 核 N 是非平凡的. 注意到事实, 如果 H 是 G 的非平凡子群, 则 G 不能被 H 的所有共轭子群覆盖. 即

$$G \neq \bigcup_{g\in G} gHg^{-1}$$

故 $N \neq \{1\}$ 是非平凡的.

(3) 对于传递的 $G-$ 集 X 而言, 任选 $x \in X$ 为轨道代表元. 我们可以利用 Frobenius 核 N 及 Frobenius 补 $H = G_x$(如果 G 是 Frobenius 群), 对有限群 G 拆解成如下结构的不交并:

$$\begin{aligned} G &= \{1\} \bigcup N^\sharp \bigcup \left(\bigcup_{g\in G} gG_x^\sharp g^{-1} \right) \\ &= \{1\} \bigcup N^\sharp \left(\bigcup_{g\in G} gH^\sharp g^{-1} \right) \end{aligned}$$

对于 Frobenius 群, 我们 Frobenius 补和 Frobenius 核有如下数量关系.

性质 6.10.26. *G 为 Frobenius 群, H 为 Frobenius 补, N 为 Frobenius 核, 则*

$$\mid N \mid = [G : H]$$

证明. **断言: Frobenius 群的 Frobenius 补 H 是自正规的 (self—normalizing)**:

$$N_G(H) = H$$

如果 $g \notin H$, 则根据定理(6.10.24), $H \cap gHg^{-1} = \{1\}$. 即 $g \notin H$, 则 $g \notin N_G(H)$. 从而 $N_G(H) \subseteq H$, 于是 $N_G(H) = H$. 因为 Frobenius 群有如下拆分:

$$G = \{1\} \bigcup N^\sharp \left(\bigcup_{g\in G} gH^\sharp g^{-1} \right)$$

故关于数量关系, 我们有如下等式:

$$\begin{aligned} \mid N \mid &= \mid N^\sharp \mid + 1 \\ &= \left(\mid G \mid - 1 + \mid \bigcup_{g\in G} gH^\sharp g^{-1} \mid \right) + 1 \\ &= \mid G \mid - (\mid H \mid - 1)[G : N_G(H)] \\ &= \mid G \mid - (\mid H \mid - 1)[G : H] \\ &= \mid G \mid - \mid H \mid [G : H] + [G : H] \\ &= [G : H] \end{aligned}$$

共轭子群彼此同构, H 的共轭子群数量为 $[G : N_G(x)]$. □

对于一般的有限群 G 而言, Frobenius 核 N 通常不是 G 的子群. 容易验证:N 对于有限群 G 的逆运算和共轭运算封闭, 即有:

$$g \in N, g^{-1} \in N$$

$$a \in G, aga^{-1} \in N$$

但是 Frobenius 核一般对于乘法运算并不封闭. 下面是一个例子.

例 6.10.27. k 为一个域, $V = k^n$ 为域 k 上的 $n-$ 维向量空间, $G = \mathrm{GL}(V)$. 类似于例子(6.10.13) $V^\sharp$ 为一个传递且忠实的左平移 $\mathrm{GL}(V)-$ 集:

$$G \times V^\sharp \longmapsto G$$

$$(A, v) \longmapsto A.v := Av$$

$A \in \mathrm{GL}(V)$ 有不动点, 当且仅当存在 $v \in V^\sharp$, $Av = v$, 当且仅当 1 为 A 的特征值. 于是, 有限群 $G = \mathrm{GL}(V)$ 的 Frobenius 核为:

$$N = \{1\} \cup \{T \in \mathrm{GL}(V) \mid T\text{不含 } 1 \text{ 为特征值}\}$$

设 $0 \neq \alpha \in k$, 满足 $\alpha^2 \neq \{1\}$. 考虑矩阵 A, B 如下:

$$A = \begin{bmatrix} \alpha, 0 \\ 0, \alpha \end{bmatrix} \in N$$

$$B = \begin{bmatrix} \alpha^{-1}, 0 \\ 0, \alpha \end{bmatrix} \in N$$

$$AB = \begin{bmatrix} 1, 0 \\ 0, \alpha \end{bmatrix} \notin N$$

于是有限群 $G = \mathrm{GL}(V)$ 的 Frobenius 核 N 不是 G 的子群. 注意到, $G = \mathrm{GL}(V)$ 不是严格双传递的, 从而不是 Frobenius 群.

注 88. 注意到, 上述例子中 $G = \mathrm{GL}(V)$ 不是 Frobenius 群. 如果有限群 G 是 Frobenius 群, 则 Frobenius 核 N 是 G 的正规子群. 这就是 Frobenius 定理, 使用有限群复表示特征标理论是此定理目前所知的唯一证明方法.

G 是一个有限群, H 是 G 的子群, ψ 是子群 H 的复特征标. 我们前面已经指出, ψ 所诱导的 G 上的特征标 $\psi\,1^G$ 在子群 H 上的限制未必是 ψ; 也就是说, ψ 所诱导的 G 上的特征标 $\psi\,1^G$ 不是由子群 H 上的复特征标 ψ 扩充得到的. 但如果 G 是 Frobenius 群, 对于 G Frobenius 补 H 上的不可约复表示 ψ 而言, 其诱导的 G 上特征标 $\psi\,1^G$ 是由 ψ 延拓扩充得到的.

性质 6.10.28. *G 为 Frobenius 群, H 为 Frobenius 补, N 为 Frobenius 核. 对于 H 上的每一个非平凡不可约复特征标 ψ, 定义 H 上的广义特征标:*

$$\varphi := \psi - d\psi_1$$

其中, $d = \psi(1) = \deg(\psi)$, ψ_1 为 H 上的平凡不可约复特征标. 令

$$\psi^* = \varphi\uparrow^G + d\mathcal{X}_1$$

其中 $\mathcal{X}_1$ 是 G 的平凡不可约复特征标. 则 ψ^* 是 G 的不可约复特征标, 且 ψ^* 是由 ψ 扩充得到的. 即对于任意的 $h \in H$,

$$\psi^*(h) = \psi(h)$$

证明. 我们将证明分成以下三个步骤进行:

(1) $(\varphi\uparrow^G)_H = \varphi$. 设 $t_1 = 1, t_2, \cdots, t_n$ 是群 G 关于子群 H 在 G/H 的左陪集代表元. 设 σ 为群 G 上特征标 $\varphi\uparrow^G$ 对应的复表示. 根据诱导特征标的计算公理(6.10.20), 对于任意的 $g \in G$:

$$\sigma(g) = \begin{pmatrix} \dot{B}(t_1^{-1}gt_1) & \dot{B}(t_1^{-1}gt_2) & \dots & \dot{B}(t_1^{-1}gt_n) \\ \dot{B}(t_2^{-1}gt_1) & \dot{B}(t_2^{-1}gt_2) & \dots & \dot{B}(t_2^{-1}gt_n) \\ \vdots & \vdots & \ddots & \vdots \\ \dot{B}(t_n^{-1}gt_1) & \dot{B}(t_n^{-1}gt_2) & \cdots & \dot{B}(t_n^{-1}gt_n) \end{pmatrix}$$

其中,

$$\dot{B}(g) = \begin{cases} 0, & g \notin H \\ B(g), & g \in H \end{cases}$$

对于任意的 $h \in H$, 因为 H 是自正规的, 则对于 $i \neq 1$, $t_i^{-1}ht_i \notin H$, 于是 $\dot{B}(t_i^{-1}ht_i) = 0$. 所以,

$$\varphi\uparrow^G(h) = \mathrm{tr}(\sigma(h)) = \mathrm{tr}(\dot{B}(h)) = \mathrm{tr}(B(h)) = \varphi(h)$$

于是,

$$(\varphi\uparrow^G)_H = \varphi$$

(2) 对于 ψ^* 满足:$(\psi^*, \psi^*) = 1$. 根据 Frobenius 互反律(6.10.20)以及 ψ 与 ψ_1 不可约特征标正交性有:

$$\begin{aligned} (\varphi\uparrow^G, \varphi\uparrow^G)_G &= (\varphi, (\varphi\uparrow^G)_H)_H \\ &= (\varphi, \varphi)_H \\ &= (\psi - d\psi_1, \psi - d\psi_1)_H \\ &= (\psi, \psi) + d^2(\psi_1, \psi_1)_H \\ &= 1 + d^2 \end{aligned}$$

类似的, 根据 Frobenius 互反律(6.10.20):

$$\begin{aligned}(\varphi\uparrow^G, \mathcal{X}_1)_G &= (\varphi, \mathcal{X}_1\downarrow_H)_H\\ &= (\varphi, \psi_1)_H\\ &= (\psi - d\psi_1, \psi_1)\\ &= -d\end{aligned}$$

于是,

$$\begin{aligned}(\psi^*, \psi^*) &= (\varphi\uparrow^G + d\mathcal{X}_1, \varphi\uparrow^G + d\mathcal{X}_1)\\ &= (\varphi\uparrow^G, \varphi\uparrow^G) + 2d(\varphi\uparrow^G, \mathcal{X}_1) + d^2(\mathcal{X}_1, \mathcal{X}_1)\\ &= 1 + d^2 - 2d * d + d^2\\ &= 1\end{aligned}$$

(3) $\psi^*(1) = \psi(1) > 0$. 根据 (1), $1 \in H$, $(\varphi\uparrow^G)_H = \varphi$. 故有:

$$\psi^*(1) = \varphi\uparrow^G(1) + d\mathcal{X}_1 = \varphi(1) + d\psi_1(1) = \psi(1) > 0$$

最后, 根据有限群广义复特征标的不可约性判别准则(6.6.10), ψ_1 是有限群 G 的不可约复特征标, 且

$$(\psi^*)_H = (\varphi\uparrow^G)_H + d(\mathcal{X}_1)_H = \varphi + d\psi_1 = \psi$$

□

下面, 我们介绍 Frobenius 定理, 并利用有限群常表示特征标理论给出其证明.

定理 6.10.29 (Frobenius 定理)**.** *G 为 Frobenius 群, H 为 Frobenius 补, N 为 Frobenius 核. $N \triangleleft G$ 是 G 的正规子群, 且 $N \cap H = \{1\}$, $G = NH$.*

注 89. 对于一般的群 G, 如果存在正规子群 $K \triangleleft G$ 以及子群 $K \leqslant G$, 使得 $K \bigcap Q = \{1\}$ 且 $G = KQ$. 则称 KQ 为群 G 的**半直积 (semiproduct)**, 称群 G 具有半直积分解. 半直积结构是群上同调论的重要研究结构和基本语言.

证明. 我们将定理的证明分成四个步骤进行:

(A) **Frobenius 群的 Frobenius 核的第三种形式—Frobenius 补上所有非平凡不可约表示的诱导特征标的核之交.** 下面, 我们构造正规子群 N^*: 因为 $H \leqslant G$, 对于 H 上的任何非平凡不可约特征标 ψ, 令

$$\varphi := \psi - d\psi_1$$

其中, $d = \psi(1) = \deg(\psi)$, ψ_1 为 H 上的平凡不可约复特征标. 令

$$\psi^* = \varphi\uparrow^G + d\mathcal{X}_1$$

其中 $\mathcal{X}_1$ 是 G 的平凡不可约复特征标. 根据性质(6.10.28), ψ^* 为群 G 的不可约复表示. 令

$$N^* = \bigcap_{\psi \neq \psi_1} \mathrm{Ker}(\psi^*)$$

显然 $N^* \triangleleft G$ 是群 G 的正规子群.

(B) **断言:**$N = N^*$**.**

(a) $N \subseteq N^*$. 首先注意到 $1 \in N^* = \bigcap_{\psi \neq \psi_1} \mathrm{Ker}(\psi^*)$. 对于任意的 $g \in N^\sharp$, 注意到

$$N^\sharp = \left(G - \bigcup_{g \in G} gHg^{-1} \right)$$

所以对于任意的 $a \in G$, $g \notin aHa^{-1}$. 对于 H 上任意的非平凡不可约复表示 ψ, 根据诱导特征标的计算公理(6.10.20)及性质(6.10.28):

$$\psi^*(g) = \varphi \uparrow^G (g) + d\mathcal{X}_1(g) = 0 + d * 1 = d = \psi(1) = \psi^*(1)$$

(b) $H \cap N^* = \{1\}$. 设 $h \in H \cap N^* = \{1\}$, 因为 $h \in H$, 根据性质(6.10.28)知: 对于 H 上任意的非平凡不可约复表示 ψ,

$$\psi^*(h) = \psi(h)$$

又因为 $h \in N^*$, 则

$$\psi^*(h) = \psi^*(1) = \psi(1)$$

于是, $\psi(h) = \psi(1)$, 故 $h \in \mathrm{Ker}(\psi)$. 考虑子群 H 上的正则表示 ρ 提供的正则特征标 $\mathcal{X}_\rho$. 因为有限群复表示是完全可约的, 故根据性质(6.6.4), 每个复表示 (复特征标) 均可表示成不可约复表示 (复特征标) 的线性组合. 设 H 的不可约复特征标为 $\psi_1, \psi_2, \cdots, \psi_r$, 其中 $d_i = \deg(\psi_i)$, 则存在不全为 0 的非负整数 $n_1, n_2, \cdots, n_r$, 使得:

$$\mathcal{X}_\rho = \sum_{i=1}^{r} n_i \psi_i$$

所以,

$$\mathcal{X}_\rho(h) = \sum_{i=1}^{r} n_i \psi_i(h) = \sum_{i=1}^{r} n_i d_i \neq 0$$

根据正则表示的性质,

$$\mathcal{X}_\rho(h) = \begin{cases} 0 & , h \neq 1 \\ \mid H \mid & , h = 1 \end{cases}$$

于是, $h = 1$. $H \cap N^* = \{1\}$.

(c) $N^* \subseteq N$. 因为 $N^* \triangleleft G$, $H \leqslant G$, 故 $HN^* \leqslant G$. 根据 Frobenius 群 G 的 Frobenius 核 N 与 Frobenius 补 H 的数量关系(6.10.26)知:

$$| N |= [G : H]$$

所以,

$$| G |=| H | [G : H] =| H || N |$$

根据群的第二同构定理,

$$HN^*/N^* \cong H/(H \cap N^*)$$

于是存在数量关系:

$$| HN^* || H \cap N^* |=| H || N^* |$$

注记: 事实上, 对于一般子群 H, K, 上式也成立:

$$| H \cap K |= \frac{| H || K |}{| HK |}$$

因为 $H \cap N^* = \{1\}$, 故 $| HN^* |=| H || N^* |$. 因为 $HN^* \leqslant G$, 故:

$$| G |=| H || N |\geqslant| HN^* |=| H || N^* |$$

于是 $| N |\geqslant| N^* |$, 结合 $N \subseteq N^*$ 知:

$$N = N^*$$

(C) 根据 (B) 及 (B) 中断言 (b), $N = N^*$, 且 $H \cap N^* = \{1\}$, 故 $H \cap N = \{1\}$.

(D) 根据 (B) 及 (B) 中断言 (c) 的证明过程知, $N = N^*$, 则 $HN = HN^* \leqslant G$ 又因为 $| G |=| H || N |$. 故 $G = HN$.

□

Frobenius 定理给出了 Frobenius 群结构的半直积表示, 同时也给出了 Frobenius 群的 Frobenius 核的第三种形式—Frobenius 补上所有非平凡不可约表示的诱导特征标的核之交. Frobenius 群有更丰富的结构性质, 例如:

(1) Frobenius 群的 Frobenius 补的每一个 Sylow 子群要么为循环群, 要么是广义四元数群 (generalized quaternion).

(2) Frobenius 群的 Frobenius 补的 Sylow 子群的上述性质是 Thompson 定理 (注记(86))"如果有限群 H 存在无不动点的素数阶自同构, 则 H 为幂零群" 的重要结果之一. 而根据幂零群的等价刻画(5.2.8), 幂零群是 Sylow 子群的直积. 故 Frobenius 核是一些循环群和广义四元数群的直积.

[12] [11] [10] [15] [14] [17] [4] [2] [8] [6] [19] [20] [18] [23] [22] [5] [7] [1] [9] [16] [13] [21] [3]

参考文献

[1] Paolo Aluffi. Algebra: Chapter 0. American Mathematical Society, 2009.

[2] Macdonald Atiyah. Introduction to Commutative Algebra. Addison—Wesley Publishing Company, 1969.

[3] Jiping Zhang Christine Bessenrodta, Hung P.Tong-Viet. Huppert' s conjecture for alternating groups. Journal of Algebra, 2017.

[4] David A. Craven. Representation Theory of Finite Groups: a Guidebook. Springer, 2019.

[5] Bruce E.Sagan. The Symmetric Group Representation, Combinatorial Algorithms, and Symmetric Functions. Springer, 2000.

[6] Brian C. Hall. Lie Groups, Lie Algebras, and Representations; An Elementary Introduction. Springer, 2015.

[7] Robin Hartshorne. Algebraic Geometry. Springer, 1997.

[8] James E. Humphreys. Introduction to Lie Algebras and Representation Theory. Springer, 1972.

[9] Daniel Simson Ibrahim Assem. Elementary of the Representation Theory of Associative Algebras, Volume 1 Techniques of Representation Theory. Cambridge University Press, 2006.

[10] Joseph J.Rotman. Advanced Modern Algebra, Part 1. American Mathematical Society, 2015.

[11] Joseph J.Rotman. Advanced Modern Algebra, Part 2. American Mathematical Society, 2015.

[12] Joseph J.Rotman. An Introduction to Homological Algebra. Springer, 2015.

[13] Mark J. Wildon Karin Erdmann. Introduction to Lie Algebras. Springer, 2010.

[14] Jean-Pierre Serre. Linear Representations of Finite Groups. Springer, 1977.

[15] P.J.Hilton; U. Stammbach. A Course in Homological Algebra. Springer, 1998.

[16] Loring. Tu. An Introduction to Manifolds. Springer, 2010.

[17] Peter Webb. A Course in Finite Group Representation. Cambridge University Press, 2016.

[18] 丘维声. 高等代数. 清华大学出版社, 2010.

[19] 丘维声. 近世代数. 北京大学出版社, 2015.

[20] 刘绍学. 近世代数基础. 高等教育出版社, 1999.

[21] 姚慕生和吴泉水. 高等代数学. 复旦大学出版社, 2016.

[22] 章璞和吴泉水. 基础代数学讲义. 高等教育出版社, 2018.

[23] 马中骐. 物理学中的群论. 科学出版社, 2006.