抽象代数笔记
群论: 反顾

EndlieDownAHell

2023 年 4 月 29 日

范畴论 DLC

函子

范畴 A,B 间的一个对应法则 F 被称为 A,B 间的一个共变函子, 若我们能从左边的图表得到右边的图表:

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

特殊的, 我们要求 $F(\mathrm{id}_A)=\mathrm{id}_{F(A)}$.

相反的, 假若我们能从如下左边的图表得到右边的图表, 称 F 为 A,B 间的反变函子:

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

自然, Grp 到 Set 的忘却函子是一个共变函子.

对于范畴 C 上的对象 A, 取定 $\mathrm{Hom}(A,X)$ 为对象, 其上的映射为态射, 生成范畴 C_A, 称为切片范畴, C 与 C_A 间的一个共变 M_A 函子可定义如下:

$$M_A(X)=\mathrm{Hom}(A,X)$$

$$\mathrm{for} f:X\to Y, M_A(f):\mathrm{Hom}(A,X)\to\mathrm{Hom}(A,Y), g\to g\circ f$$

同样的, 对于范畴 C 上的对象 A, 取定 $\mathrm{Hom}(X,A)$ 为对象, 其上的映射为态射, 生成范畴 C^A, 称为余切范畴, C 与 C^A 间的一个反变 M^A 函子可定义如下:

$$M^A(X)=\mathrm{Hom}(X,A)$$

$$\mathrm{for} f:X\to Y, M^A(f):\mathrm{Hom}(X,A)\to\mathrm{Hom}(Y,A), g\to f\circ g$$

例 1 按照如下方法从诱导出 Grp 到 Ab 的一个共变函子:

$$\begin{tikzcd}
G \arrow[r, "\varphi_G"] \arrow[d, "f"'] & G/[G,G] \arrow[d, "\tilde{f}"] \\
H \arrow[r, "\varphi_H"] & H/[H,H]
\end{tikzcd}$$

对于 A, B 及其间的函子 L, M, 取定 Ob(A) 上的一个对应 η, 这对应为 A 上的一个对象 X 指定了一个将 $L(X)$ 指向 $M(X)$ 的态射 η_X, 使得下面的图表交换:

$$\begin{tikzcd}
L(X) \arrow[r, "\eta_X"] \arrow[d, "L(f)"'] & M(X) \arrow[d, "M(f)"] \\
L(Y) \arrow[r, "\eta_Y"] & L(Y)
\end{tikzcd}$$

这对应被我们称为函子 L 到 M 的一个自然变换.

例 2 取定范畴 A, B 间所有的共变函子为对象, 函子间的自然变换为态射, 查看下面的图表交换:

$$\begin{tikzcd}
L(A) \arrow[r, "\eta_A"] \arrow[rr, bend left, "\rho_A\eta_A"] \arrow[d, "L(f)"] & M(A) \arrow[r, "\rho_A"] \arrow[d, "M(f)"] & K(A) \arrow[d, "K(f)"] \\
L(B) \arrow[r, "\eta_B"] \arrow[rr, bend right, "\rho_B\eta_B"'] & M(B) \arrow[r, "\eta_B"] & M(B)
\end{tikzcd}$$

于是这是一个范畴.

积与余积

取定范畴 A 的一族对象 $\{A_{i\in I}\}$, 这族对象的积 $(P, \{f_{i\in I}\})$ 是 A 的对象 P 与其上的一个态射族 $\{f_{i\in I}\}$, 使得如下图表交换:

$$\begin{tikzcd}
C \arrow[r, dashed] \arrow[d, "g_i"'] & P \arrow[dl, "f_i"] \\
A_i &
\end{tikzcd}$$

其中 C 是任意 A 中对象, $\{g_{i\in I}\}$ 成一态射族.

取定范畴 A 的一族对象 $\{A_{i\in I}\}$, 这族对象的余积 $(P, \{f_{i\in I}\})$ 是 A 的对象 P 与其上的一个态射族 $\{f_{i\in I}\}$, 使得如下图表交换:

$$\begin{tikzcd}
C & P \arrow[l, dashed] \\
A_i \arrow[u, "g_i"] \arrow[ur, "f_i"] &
\end{tikzcd}$$

其中 C 是任意 A 中对象, $\{g_{i\in I}\}$ 成一态射族.

自由群

这一节讲得不是很好, 建议看其他的材料, 完全从泛性质出发构架自由群不是不行, 但是具体构造过程不做一点解释 (明明完全可以和数理逻辑结合得很好的) 只会和高等线性代数讲的张量积一样上不去也下不来, 造成很坏的影响.

建议先查看定理四的证明对本节一些迷惑行为的解读再读其他内容.

自由群

取定集合 S 与群 G, 假若映射 f 能够使得

$$\langle f(S)\rangle = G$$

称 f 生成了 G.

定义 1 取定集合 S, 若有 S 上映射生成了群 F, 对于任意的群 G 使得下图交换, 称 (F, f) 是 G 确定的自由群:

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d, "g"'] & F \arrow[dl, dashed, "h"] \\ G & \end{tikzcd}$$

其中 h 是群同态.

下面引入群积的概念, 对自由群的存在性进行一些说明:

定义 2 为群族 $\{G_{i\in I}\}$ 的笛卡尔积 $\prod\limits_{i\in I} G_i = (x_{i\in I}), x_i \in G_i$ 定义运算

$$(x_{i\in I})(y_{i\in I}) = (xy_{i\in I})$$

称为这族群的积, 容易证明 $\prod\limits_{i\in I} G_i$ 联合诸投影映射 π_i 便是 $\{G_{i\in I}\}$ 在 Grp 上的积, 另外的, 取定同态

$$\lambda_i : G_i \to \prod_{i\in I} G_i, g \to (e_1, \cdots, e_{i-1}, g, e_{i+1}, \cdots)$$

即刻能够确信一组 $G'_{i\in I}$ 的存在, 满足:

$$G'_i \simeq G_i, \prod_{i\in I} G_i = \bigotimes_{i\in I} G'_i$$

等式右边是群直积.

特殊的, λ_i 这种将小结构 G_i 保持结构嵌入大结构 $\prod\limits_{i\in I} G_i$ 的单同态被称为自然嵌入.

引理 1 取定集合 S, 存在着群族 $G_{i\in I}$, 若 S 上映射 g 将 G 生成, 总有 $\{G_{i\in I}\}$ 中成员使得 $G \simeq G_i$

Proof. S 为有限集时, g 生成的群自然是至多可数的, S 为无限集时, 其生成的集合 G 由于可表为 $g(S)$ 及其逆的有限积, 从而 $|G| \leq |S|$.

对于有限的 S, 取定可数集 T 作为其可能的字符组合的全体 (反正能对应起来), 对于无限的 S, 取定 $|T| = |S|$ 作为字符组合的全体, 为任意 $H \subset T$ 指派 Γ_H 为 H 上群结构的全体 (注意到这群结构完全由运算表 $ab = c$ 决定), 要求 H_γ 是 $\gamma \in \Gamma$ 在 H 上作用的结果, 现在,

$$\{H_\gamma \mid H \subset T, \gamma \in \Gamma_H\}$$

便是我们所需要的. □

定理 2 针对集合 S 总存在相应的自由群 (F, f).

Proof. 我们自然能够把 S 上映射 g 生成的群 G 归入群族 $\{G_{i\in I}\}$ 中, 针对这群族中的 G_i, 生成映射族如下:

$$M_i = \{\varphi \mid \varphi : S \to G_i\}$$

利用 $\varphi \in M_i$ 将 G_i 标记, 得到一组实际上无差然而下标各异的群族 $\{G_{\varphi\in M_i}\}$, 以次得到群积及相应的映射如下[1]:

$$F_0 = \prod_{i\in I \varphi_i\in M_i} G_{i,\varphi}, f_0 : S \to F_0, s \to (\overrightarrow{\varphi_i(s)}_{i\in I})$$

这群对命题的证明而言, 仍旧是过大的, 我们现在来做一点修剪的工作:

$$F = \langle f_0(S)\rangle, f : S \to F, s \to f_0(s)$$

考虑 S 与任意群 G 之间的映射 g, 不妨假定 g 将 G 生成, 否则在 $\langle f(S)\rangle < G$ 中讨论问题, 依照引理 1, 立即可以取定 G_i 及同构映射 $\lambda : G \to G_i$, 此时 $\varphi = \lambda \circ g$ 是 $S \to G_i$ 的一个映射, 因而存在于 M_i 中, 便能在生成 F_0 的一众集合中取定 $G_{i,\varphi}$ 以及相应的投影 $\pi_{i,\varphi}$, 也即是如下图左的交换图:

$$\begin{tikzcd} S \arrow[r, "f_0"] \arrow[d, "g"'] \arrow[dr, "\varphi"] & F_0 \arrow[d, "\pi_{i,\varphi}"] \\ G \arrow[r, "\lambda"] & G_{i,\varphi} \end{tikzcd} \qquad \begin{tikzcd} S \arrow[r, "f_0"] \arrow[d, "g"'] & F_0 \arrow[d, "\pi_{i,\varphi}"] \arrow[dl, "\varphi^*"'] \\ G & G_{i,\varphi} \arrow[l, "\lambda^{-1}"] \end{tikzcd} \qquad \begin{tikzcd} S \arrow[r, "f"] \arrow[d, "g"'] & F \arrow[d, "\pi_{i,\varphi}"] \arrow[dl, "h"'] \\ G & G_{i,\varphi} \arrow[l, "\lambda^{-1}"] \end{tikzcd}$$

考虑到 λ 作为同构的可逆性, 从左图便可得到中间的交换图, 再取定 $h = \varphi^* |_F$, 则这交换图依照 $\forall s \in S, f(s) = f_0(s)$ 还可改写为右边的图. h 便是自由群定义中所需要的群同态, 假定再有其他 h' 满足条件, 将存在下图左的交换图:

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d, "g"'] & F \arrow[dl, "h'"'] \\ G \arrow[r, "\lambda"] & G_{i,\varphi} \arrow[u, "\iota"'] \end{tikzcd} \qquad \begin{tikzcd} S \arrow[r, "f"] \arrow[d, "g"'] & F \arrow[d, "\pi_{i,\varphi}"] \arrow[dl, "h'"'] \\ G & G_{i,\varphi} \arrow[l, "\lambda^{-1}"] \end{tikzcd}$$

从左边的交换图, 不难确定右边的图表交换, 于是 $h = h'$, 唯一性得证. □

[1]庆幸一下你看到了这条脚注, 以后的笔记我都会用 overrightarrow 表示序列: $\overrightarrow{x} = (x_1, \cdots, x_n)$, 是否再做注释完全看心情.

考虑到 f 是单射, 进行简单的字母替换后, 我们自然可以声称 $F=\langle S\rangle$, 此时我们称 S 是 F 的自由生成元, 这自由生成元的生成的自由群于是也可反向地记为 $F(S)$, 相应的映射为 f_S, 现在查看如下的交换图:

$$\begin{tikzcd}
S \arrow[r, "f_S"] \arrow[d, "\lambda"'] \arrow[dr, "f_{S'}\circ\lambda"] & F(S) \arrow[d, dashed, "F(\lambda)"] \\
S' \arrow[r, "f_{S'}"] & F(S')
\end{tikzcd}$$

其中 $F(\lambda)$ 的唯一指派是自由群 $F(S)$ 的泛性质的结果. 查看下面的交换图:

$$\begin{tikzcd}
S_3 \arrow[rrr, "f_{S_3}"] & & & F(S_3) \\
& S_2 \arrow[ul, "\lambda"] \arrow[r, "f_{S_2}"] & F(S_2) \arrow[ur, dashed, "F(\lambda)"] & \\
S_1 \arrow[uu, "\lambda\circ\mu"] \arrow[ur, "\mu"] \arrow[rrr, "f_{S_1}"] & & & F(S_1) \arrow[ul, dashed, "F(\mu)"] \arrow[uu, dashed, "F(\lambda)\circ F(\mu)"']
\end{tikzcd}$$

$$\begin{tikzcd}
S_1 \arrow[r, "f_{S_1}"] \arrow[d, "\lambda\circ\mu"'] \arrow[dr, "\varphi"] & F(S_1) \arrow[d, dashed, "F(\lambda)\circ F(\mu)"] \\
S_3 \arrow[r, "f_{S_3}"] & F(S_3)
\end{tikzcd}
\qquad
\begin{tikzcd}
S \arrow[r, "f_S"] \arrow[d, dash, "\mathrm{id}_S"'] \arrow[dr] & F(S) \arrow[d, dash, dashed, "\mathrm{id}_{F(S)}"] \\
S \arrow[r, "f_S"] \arrow[ur] & F(S)
\end{tikzcd}$$

上方的交换图表对 F 构成 Set, Grp 间函子进行了说明, $F(\lambda\circ\mu)=F(\lambda)\circ F(\mu)$ 的成立只需对左下的图表进行考察, 注意 $F(S_1)$ 的泛性质即可, $F(\mathrm{id}_S)=\mathrm{id}_{F(S)}$ 这一要求, 从右下的图表已经是十分显然的了.

如上结果向我们预示着假若 $|S_1|=|S_2|$, 将有 $F(S_1)\simeq F(S_2)$, 故而自由群的区别仅在于生成元集的阶, 当其有限时, 我们称之为具有 n 个生成元的自由群.

定理 3 任意群总是某个自由群的商群.

Proof. 查看如下的交换图:

$$\begin{tikzcd}
G \arrow[r, "f_S"] \arrow[d, "\mathrm{id}_G"'] & F(G) \arrow[dl, dashed, "h"] \\
G &
\end{tikzcd}$$

注意到 id_G 为满射, 故 h 必然是满同态, 此时自然成立:

$$G\simeq F(S)/\mathrm{Ker}(h)$$

□

这为我们提供了一种描述与构造群的思路, 即使用生成元生成自由群, 再利用生成元间额外的谓词对自由群进行修剪 (实际上是商去这满足这关系的元素生成的正规子群), 例如在 a 生成的自由群 F 上使用谓词 $a^m=e$, 于是在这额外追加的谓词下, F 便被修剪为了 C_m.

定理 4 Grp 中总存在一族群 $\{G_{i\in I}\}$ 的余积.

Proof. 对有限的 G_i 取定 S_i 作为其可能的字符组合的集合, 也即我们并不关心对于 $x_1, x_2 \in G_i$ 而言 x_1x_2 究竟指向何物, 而仅是形式地将其记为 x_1x_2 这个字符串, 类似的字符串还有

$$xxxyyy, x^{-1}yyx, x_1x_1x_4x_5x_1x_4$$

S_i 的内容物本应就是这些字符串, 然而考虑到 S_i 反正是个可数集, 随便取一个可数集就好, 反正都能建立 1-1 的对应, 正所谓所有人都不认识你的时候, 你是叫何塞 · 阿尔卡蒂奥 · 布恩迪亚还是叫键山雏都无所谓了, 类似的, 我们为无限的 G_i 施加大遗忘函子使其变为任何仅仅是与 G_i 等势的一般通过麻瓜集合 S_i, 现在构造集合[1]

$$S = \bigsqcup_{i\in I} S_i$$

现在令 Γ 是 S 上所有可行的群结构 γ 的组合 (注意到确定这个群结构只需要给定个运算表说明 ab 被指到什么勾 8 地方就行[2]) 将各种 γ 生成的别有千秋妙趣横生的群记为 S_γ 以示区分.

现在遍历 G_i 到特定的 S_γ 的同态, 对于某一个同态 $\varphi_i : G_i \to S_\gamma$, 记载一个 S_{γ,φ_i}, 尽管其与 S_γ 没什么区别, 然而这种事情就和结绳记事, 石头计数和 Lex 直播嗷嗷哭一样无脑, 野蛮且实用[3]现在再把 S_γ 上能施加的类似傻卵同态归成 $\varPhi_\gamma$ 我们便能生成如下一个乱动的大图书馆:

$$F_0 = \prod_{\gamma\in\Gamma, \varphi\in\varPhi_\gamma} S_{\gamma,\varphi}$$

这图书馆记载了群 G_i 的群胚作为生成元都能生成哪些和这节的符号体系一样唐氏的群, 具体的查找目录是如下的一个同态:

$$f_i : G_i \to F_0, s \to \overrightarrow{\varphi_i(s)}$$

针对 $g : G_i \to G$, 若 G 恰好与 S 这种缝合奇美拉等势自然皆大欢喜, 否则变为 $S \times \mathbb{Z}^n$ 与 S 同势, 反正最后还有唯一的同态变回来 (因而也暂时记后者为 G), 现在, 不妨假定 g 生成了 G, 否则就在子群 $\langle g(G_i) \rangle$ 中讨论这个问题, 在这个与 S 等势的群 G 自然可以视为负载了某种群结构的 S_γ, 于是 g 也便是 $\varPhi_\gamma$ 中的某个逆天, 自然的, 投影映射 π_{G_g} 便使得下面的交换图交换:

$$\begin{tikzcd} G_i \arrow[r, "f_i"] \arrow[d, "g"'] & F_0 \arrow[dl, "\pi_{G_g}"] \\ G & \end{tikzcd} \qquad \begin{tikzcd} G_i \arrow[r, "f_i"] \arrow[d, "g"'] & F \arrow[dl, dashed, "\pi_{G_g}"] \\ G & \end{tikzcd}$$

由于我们并不关心 F_0 中诸如 $(\overline{\varphi(s)}, \overline{\varphi(t)})$ 一类的让纯爱战士想起 NTR 剧情的坷拉琪元素, 我们将其修剪为 $F = \left\langle \bigcup_{i\in I} \mathrm{im} f_i \right\rangle$, 于是得到了右边的交换图, 现在, F 联合诸多 f_i 便是我们所需要的余积. $\square$

[1]考虑到你们应该都在我之前的文章里面听 Chapter 0 嬷嬷讲过无交并的故事了, 我这里也就不多废话了

[2]实际上给个 S 到自身的映射就行, 反正 $p, q \in S$ 的组合结果 pq 就在 S 里面

[3]我要是直播嗷嗷哭就能挣买数理逻辑导引的米我早退学当皮套人去了.

定理 5 针对任意集 S, 存在被 S 确定的自由 Abel 群.

Proof. 取定映射集如下:

$$\mathbb{Z}(S) = \{\varphi : S \to \mathbb{Z} \mid 仅有有限个x \in S使得\varphi(x) \neq 0\}$$

在 $\mathbb{Z}(S)$ 上定义加法为 $\varphi + \psi : x \to \varphi(x) + \psi(x)$, 于是 $\mathbb{Z}(S)$ 自成一 Abel 群, 定义简单映射 $k \circ x$ 如下:

$$k \circ x : S \to \mathbb{Z}, s \to \begin{cases} k, s = x \\ 0, s \neq x \end{cases}$$

于是 $\varphi(x)$ 总可被唯一 (实际上有限) 地表为:

$$\varphi = \sum_{x \in S} \varphi(x) \circ x$$

表法的唯一性只在于 $0 : x \to 0$ 的表法唯一.

现在取定 f 为 $f : S \to \mathbb{Z}, x \to 1 \circ x$, 自然 f 单且生成了 $\mathbb{Z}(S)$, 对于其他的 Abel 群 A, 取定映射 $h : \mathbb{Z}(S) \to A, \sum_{x \in S} \varphi(x) \circ x \to \sum_{x \in S} \varphi(x) g(x)$, 自然有如下交换图成立:

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d, "g"'] & \mathbb{Z}(S) \arrow[dl, dashed, "h"] \\ A & \end{tikzcd}$$

对于唯一性的成立, 只需注意到 $\mathbb{Z}(S)$ 与 A 间同态 $\mathfrak{h}$ 需要满足:

$$\mathfrak{h}\left(\sum_{x \in S} \varphi(x)\right) \circ x \to \sum_{x \in S} \varphi(x) \mathfrak{h}(x)$$

而使得图表交换的 $\mathfrak{h}$ 应当将众 $x \in S$ 送向何处已经是板上钉钉的事情了. $\square$

与自由群类似的, 针对自由 Abel 群有如下的一些结论:

(i) 存在由自由 Abel 群导出的 Set 到 Ab 间的函子.

(ii) $|S| = |S'|$, 则 $F_{Ab}(S) \simeq F_{Ab}(S')$

(iii) Abel 群总同构于自由 Abel 群的某个商群.

将 Abel 群族 $\{A_{i \in I}\}$ 在 Ab 中的余积称为直和.

定理 6 Ab 中直和存在.

Proof. 取定 Abel 群族 $\{A_{i \in I}\}$, 令

$$A = \left\{ (x_{i \in I}) \in \prod_{i \in I} A_i \mid 仅有有限个x_i \neq 0 \right\}$$

自然 $A < \prod_{i \in I} A_i$, 取定 λ_i 是 A_i 到 A 的嵌入, 对于 Abel 群 $\mathcal{A}$, 存在如下的交换图表:

$$\begin{tikzcd} A_i \arrow[r, "\lambda_i"] \arrow[d, "g"'] & A \arrow[dl, dashed, "f"] \\ \mathcal{A} & \end{tikzcd}$$

其中 f 按照下式规定:

$$f(\overrightarrow{x_{i\in I}}) = \sum_{i\in I} g(x_i)$$

要求了 $\overrightarrow{x_{i\in I}}$ 有限, 于是这和是能做到的, 不难验证 $f\circ\lambda_i$, 同样是不妨假定 g 生成了 $\mathbb{A}$, 否则就在子群中完成讨论, 与定理 6 一致的理由, f 的唯一性成立. $\square$

定理 7 针对交换幺半群 M, 存在 Abel 群 $K(M)$ 与幺半群同态 γ, 使得如下图表对任意的 Abel 群 D 与幺半群同态 β 成立:

$$\begin{tikzcd}
M \arrow[r, "\gamma"] \arrow[d, "\beta"'] & K(M) \arrow[dl, dashed, "k"] \\
D &
\end{tikzcd}$$

$K(M)$ 被称为 M 的 Grothendieck 群.

Proof. 取定 $F_{Ab}(M)$, 将 $x\in M$ 在 $F_{Ab}(M)$ 中对应的字符串记为 $[x]$, 现在进行如下操作:

$$K(M) := F_{Ab}(M)/B$$

$$B = \langle \text{Cutalbe} \rangle$$

$$\text{Cutable} = \{[x+y]-[x]=[y] \mid x,y\in M\}$$

这实际上是对 $F_{Ab}(M)$ 的元素进行了约化, 将以 $[x+y]-[x]-[y]$ 为代表的一些在任何一个交换半群同态 β 中都会被指向 0 的元素合并后, 我们便得到了 $K(M)$, 现在, 查看如下交换图, 命题的成立已经不言而喻:

$$\begin{tikzcd}
F_{Ab}(M) \arrow[drr, "a\to\langle a\rangle"] & & \\
M \arrow[u, "x\to[x]"] \arrow[rr, "\gamma:x\to\langle x\rangle"] \arrow[d, "\beta"'] & & F_{Ab}(M)/B \arrow[dll, dashed, "\langle x\rangle\to\beta(x)"] \\
D & &
\end{tikzcd}$$

$\square$

命题 8 当交换幺半群 M 满足消去律时, M 到 $K(M)$ 的上述映射 γ 是单的.

Proof. 考虑为 M 上的二元组 $W=\{(x,y)\mid x,y\in M\}$ 建立如下等价关系:

$$(x,y)\sim(x',y') \Leftrightarrow x+y'=y+x'$$

应用这等价关系去商 W, 得到 Σ, 其等价类以代表元记载之, 在 W 定义如下运算,

$$\overline{x,y}+\overline{x',y'}=\overline{(x+x',y+y')}$$

这运算与 M 于是成一加法群, 所需的幺元是 $\overline{(0,0)}$, $\overline{(x,y)}$ 的逆元为 $\overline{(y,x)}$.

定义 $g : M \to \Sigma, x \to \overline{(0,y)}$, g 自然是一个单的幺半群同态, 从如下交换图, γ 为单射已经是无法避免的事情了:

$$\begin{tikzcd}
M \arrow[r, "\gamma"] \arrow[d, "g"'] & K(M) \arrow[dl, dashed, "h"] \\
\Sigma &
\end{tikzcd}$$

□

引理 9 取定 Abel 群 A 与自由 Abel 群 A' 间的满同态 f, 则存在着 A 的自由子群 F 同构于 A', 且

$$A = \mathrm{Ker} f \oplus F$$

Proof. 取定自由群 A' 的一组基 $\{x'_{i\in I}\}$, 由于 f 是满的, 能够为 x'_i 各自找到 A 上的对应 x_i 使得

$$f(x_i) = x'_i$$

考虑 $\{x_{i\in I}\}$ 的有限线性组合 (这便意味着只有有限个 k_i 是非零的):

$$\sum_{i\in I} k_i x_i = 0$$

即得下式

$$f\left(\sum_{i\in I} k_i x_i\right) = \sum_{i\in I} k_i f(x_i) = \sum_{i\in I} k_i x'_i$$

考虑到 x'_i 为自由 Abel 群 A' 的基, 便只能 $k_i \equiv 0$, 这反过来说明了 $F =\rangle\{x_{i\in I}\}\langle$ 生成的群必然无简并出现, 也即诸多有限组合的 $\sum\limits_{i\in I} k_i x_i$ 必然互不相等, 这一方面说明 F 中绝无 $\mathrm{Ker} f$ 的成员, 另一方面也与自由群逿论含义堆放符号串的作风一脉相承, 于是我们确信了 F 的自由群属性.

现在, 针对 $x \in A$, 我们总有下式:

$$f(x) = \sum_{i\in I} k_i x'_i$$

也即 $f\left(x - \sum\limits_{i\in I} k_i x_i\right) = 0$, 这便说明 $x - \sum\limits_{i\in I} k_i x_i$ 在 $\mathrm{Ker} f$ 之中, 于是命题的成立便已经十分显然了. □

定理 10 自由 Abel 群的子群依旧是自由的, 其基数不大于原来的 Abel 群, 任意两个基的基数相等.

Proof. 这定理尽管是普适的, 我们依旧仅针对有限生成的情形完成证明.

取定有限生成的自由 Abel 群 A 被表为如下形式:

$$A = \bigoplus_{i=1}^{n} \mathbb{Z} x_i$$

对 n 进行归纳, 取定 $B < A$ 及投射 $\pi_1 : A \to \mathbb{Z} x_1$, 要求 $B_1 = \mathrm{Ker}\pi_1 \mid_B$, 自然 $B_1 < \bigoplus\limits_{i=2}^{n} \mathbb{Z}_i$, 依照归纳假设 B_1 便是自由的 Abel 群, 其基不大于 $n-1$.

现在来探讨 B 的情况, $f(B) < \mathbb{Z}x_1$, 于是 $f(B)$ 要么是 $\{0\}$, 要么为一无限循环群, 若为前者, $\mathrm{Ker}\pi_1\mid_B = B$, 证明已经结束, 若为后者, 假定 $f(B) = \mathbb{Z}dx_1$, 应用引理 9, 将有一同构于 $\mathbb{Z}dx_1$ 的群 F 将 B 直和分解为:

$$B = F \oplus \mathrm{Ker}\pi_1\mid_B$$

则 B 是自由的, 且其基的个数为 $n-1+1=n$.

现在, 假定 B 有个数分别为 s, t 的基 S, T, 取定素数 p 生成 $pB \lhd B$, 于是:

$$B = \bigoplus_{i=1}^{r} \mathbb{Z}r_i = \bigoplus_{j=1}^{t} \mathbb{Z}t_j$$

$$B/pB = \bigoplus_{i=1}^{r} \mathbb{Z}_p r_i = \bigoplus_{j=1}^{t} \mathbb{Z}_p t_j$$

于是 $|B/pB| = p^r = p^t$, 便知道 $r = s$, 这为我们将自由 Abel 群的基的元素个数称为该 Abel 群的秩提供了充分的理由. $\square$

$15 \leq$ 阶的有限群分类

先来介绍两个典型群以期分解时使用:

二面体群

假定 $n \geq 3$, 应用关系 $|a| = n, b^2 = e, ba = a^{-1}b$ 约化 $\{a, b\}$ 生成的自由群, 所得的 $2n$ 阶群被称为二面体群.

显然 $\langle a \rangle \lhd D_n$, 另外的, 考虑 S_n 的两个元素:

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ n & 1 & \cdots & n-1 \end{bmatrix}, \tau = \begin{bmatrix} 1 & 2 & \cdots & n \\ 1 & n & \cdots & 2 \end{bmatrix}$$

自然 $|\sigma| = n, \tau^2 = e$, 另外的,

$$\tau\sigma = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & n & \cdots & 3 \end{bmatrix}, \sigma^{-1}\tau = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & n & \cdots & 3 \end{bmatrix}$$

于是我们确信 $D_n < S_n$.

D_2 同样是可以定义的, 然而这实际上便是 Klein 群.

四元数群

按照关系 $i^4 = j^4 = e, ji = i^3 j$ 约化 $\{i, j\}$ 生成的自由群得到的 8 阶群被称为四元数群 Q_8, 这群实际上也是

$$\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm\begin{bmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \pm\begin{bmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix}$$

注意到 D_4 中的二阶元有 b, a^2b, 而 Q_8 中的二阶元只有 $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, 于是 Q_8 并不是一个二面体群.

定理 11 阶为 p^2 的群 G 不是 C_{p^2} 就是 $C_p \times C_p$.

Proof. G 若非循环群, 自然知道其包含两个 p 阶子群 $\langle a\rangle, \langle b\rangle$, 满足着 $\langle a\rangle \cap \langle b\rangle = \{e\}$.

G 自然是一个 p 群, 于是 $\langle a\rangle, \langle b\rangle$ 各自的正规化子将其真包含, 这正规化子, 于是只能是 G, 也即 $\langle a\rangle, \langle b\rangle \lhd G$, 从而已经能够确信

$$G = \langle a\rangle \times \langle b\rangle \simeq C_p \times C_p$$

□

定理 12 取定群 G 为 pq, 其中 p, q 为素数, 满足 $p > q$, 当 $q \equiv 1 \pmod p$ 时, G 为 C_{pq}, 若 $q \mod p \neq 1$, 则 G 要么是 C_{pq}, 要么是由 p, q 生成的如下群:

$$dcd^{-1} = c^r, |c| = p, |d| = q$$

$$r \mod p = 1, r^q \equiv 1 \pmod p$$

Proof. G 的 Sylow p 群自然是一个 p 阶循环群 P, 这样的 Sylow p 群的个数 n_p, 作为 P 在 G 集 $\mathcal{P}(G)$ 的轨道阶数, 可计算为 $[G : \mathrm{St}(P)]$, 自然将 pq 整除, 然而 $n_p \equiv 1 \pmod p$, 于是只能 $n_p \mid q$, 从而 $n_p = 1$, 于是 P 共轭作用后的结果只能是 P, 这便指明了 $P \lhd G$.

再来查看 Sylow q 群 Q, 同样的, n_q 具有 $kq + 1$ 的形式且将 p 整除, 假若能够实现 $kq + 1 = p$, 按下不谈, 否则只能是 $n_q = 1$, 于是 $Q \lhd G$, 于是

$$G = P \times Q \simeq C_p \times C_q \simeq C_{pq}$$

现在考虑 $kq + 1 = p$ 的情形, 将 P, Q 改写为 $\langle c\rangle, \langle d\rangle$, Q 若正规, 转为上一种情况, 否则至少有

$$dcd^{-1} = c^r$$

此处 $r \mod p$ 自然不为 1, 否则又是 $dc = cd$, 这是上一种情况, 而考虑下面的一列式子:

$$c^{2r} = dcd^{-1}dcd^{-1} = dc^2d^{-1}$$

$$c^{r^2} = c^{r \cdot r} = dc^r d^{-1} = ddcd^{-1}d^{-1} = d^2cd^{-2}$$

于是, 我们还有

$$c = d^q c d^{-q} = c^{r^q}$$

这便意味着 $r^q \equiv 1 \pmod p$.

我们还需要反向确定这样的一组 $\langle c\rangle, \langle d\rangle, r$ 确实能够生成 pq 阶的群, 为此我们急需确定一种新的生成群的方式, 为此我们跳转到如下一个命题:

定理 13 取定群 H, K, 假若能够为 h 指定 $\mathrm{Aut}(K)$ 中的一个 I_h, 使得

$$I_{h_1} \circ I_{h_2} = I_{h_1 h_2}$$

则 $\{(h, k) \mid h \in H, k \in K\}$ 形成了具备如下一个运算的群:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, I_{h_2}(k_1)k_2)$$

这群被称为 H, K 间的半直积 $H \rtimes K$.

Proof. 验证的工作如下:

$$(h_1,k_1)(h_2,k_2)=(h_1h_2,I_{h_2}(k_1)k_2)$$

$$(h_1h_2,I_{h_2}(k_1)k_2)(h_3,k_3)=(h_1h_2h_3,I_{h_2h_3}(k_1)I_{h_3}(k_2)k_3)$$

$$(h_2,k_3)(h_3,k_3)=(h_2h_3,I_{h_3}(k_2)k_3)$$

$$(h_1,k_1)(h_2h_3,I_{h_3}(k_2)k_3)=(h_1h_2h_3,I_{h_2h_3}(k_1)I_{h_3}(k_2)k_3)$$

$$(h,k)(e,e)=(he,I_e(k)e)=(h,k)$$

$$(h,k)(h^{-1},I_{h^{-1}}(k^{-1}))=(hh^{-1},I_{h^{-1}}(k)I_{h^{-1}}(k^{-1}))=(e,e)$$

□

请读者自己补全第五个等式缺失的一处细节.

现在, 针对 $\langle c\rangle,\langle d\rangle$ 定义如下的半直积:

$$I_{d^x}(c^y)=d^xc^yd^{-x}=c^{y^x}$$

$$(d^uc^v)(d^xc^y)=d^{u+x}c^{v^x}c^y=d^{u+x}c^{v^x+y}$$

这便能生成 pq 阶的群. □

推论 14 对于素数 p, $2p$ 阶群 G 不是 C_{2p} 就是 D_p.

定理 15 非交换的 8 阶 Abel 群只有 Q_8,D_4.

Proof. 非交换的八阶群必然存在元素的阶数为 4, 否则这群将是交换的, 取定这四阶的元 a, 不难从 $[G:\langle a\rangle]=2$ 发现 $\langle a\rangle\lhd G$, 于是知道

$$G/\langle a\rangle=\{\langle a\rangle,b\langle a\rangle\}$$

不难知道 $b^2\in\langle a\rangle$, 若 $b^2=a$, 则 $b^4\neq e,b^8=e$, 从 G 非交换这是不可能的[1]; 若 $b^2=a^3$, 同样的理由使我们确信这不可能. 另外的, $bab^{-1}\in\langle a\rangle$, 从前对 b^2 的限定, 只能是 $bab^{-1}=a^3=a^{-1}$.

现在, 若 $b^2=a^2$, 则联合 $ba=a^{-1}b$ 有 $G\simeq Q_8$, 若 $b^2=e$, 同样的我们有 $G\simeq D_4$. □

在完成 12 阶群的工作前, 我们再补充一个群的例子:

命题 16 $S_3\times C_4$ 具有一个 12 阶非交换子群 T, 其由生成元 x,y 生成, 其中 $|x|=6,x^3=y^2,yx=x^{-1}y$. 这群与 D_6 不同构.

Proof. 设定 C_4 的生成元为 c, 则所需的 x,y 可自如地验证为

$$x=((123),c^2),y=((12),c)$$

自然 $\langle y\rangle=C_4<T$, 然而 D_6 中绝无四阶循环子群, 于是 T 与 D_6 不同构. □

[1]对抱有着“万一 $b^{3,5,6}=e$ 怎么办”的疑虑的同学, 请好好想想你的 Lagrange 定理都学哪去了.

引理 17 取定 $H < G$, 若 $[G:H]=n$, 则存在同态 $G \to S_n$ 使得 $H \subset \mathrm{Ker} f$.

Proof. 用 S 表示 H 左陪集的全体, 自然 $|S|=n$, 取定 $\tau_g(xH)=gxH$, 于是 $\tau_g \in \mathrm{Aut}(S)$.

考虑到 $\mathrm{Aut}(S) \simeq S_n$, 取定其间同构映射 η, 验证如下图表交换命题自成立:

$$\begin{tikzcd} G \arrow[r, "g\to\tau_g"] \arrow[dr] & \mathrm{Aut}(S) \arrow[d, hook, two heads] \\ & S_n \end{tikzcd}$$

□

命题 18 非交换的 12 阶群, 只能是 D_6, A_4, T 中其一.

Proof. 悲报, 刚刚发现自己的某个回答火到被同学看见了, 写完致谢一样的小文章过后不想再写证明了, 反正和 8 阶的情况大差不差, 自己查资料去吧. □

现在, 我们完成了所有的分类工作, 结果汇总如下:

阶数	群
1	$\{e\}$
2,3,5,7,11,13	C_p
4,9	$C_2 \times C_2, C_4/C_3 \times C_3, C_9$
6,10,14	C_{2p}, D_p
8	$C_2 \times C_2 \times C_2, C_2 \times C_4, C_8, Q_8, D_4$
12	$C_2 \times C_6, C_{12}, A_4, D_6, T$
15	C_{15}

线性群

F 上全体 $n \times n$ 阶可逆矩阵被称为一般线性群 $\mathrm{GL}_n(F)$, 其中行列式为 1 的矩阵全体组成 $\mathrm{GL}_n(F)$ 的一个子群 $\mathrm{SL}_n(F)$, 称为特殊线性群.

定理 19

$$\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \simeq F^*$$

其中 F^* 是 F 去除零元后生成的乘法群.

Proof. 查看如下的同态:

$$\det : \mathrm{GL}_n(F) \to F^*, A \to \det A$$

自然 $\operatorname{im}\det = F^*, \operatorname{Ker}\det = \mathrm{SL}_n(F)$, 这命题便只是如下一个简单结论的结果:

$$\text{For } f : G \to H, G/\mathrm{Ker} f \simeq \mathrm{im} f$$

□

我们来探讨一番 $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$ 中等价类的代表元, 自然, $A \sim B \Leftrightarrow \det A = \det B$, 这其中的一个典型便是 $\begin{bmatrix} E_{n-1} & O \\ O & \det A \end{bmatrix}$, 也即我们可以将 $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$ 改写为:

$$\bigcup_{d \in F^*} \begin{bmatrix} E_{n-1} & O \\ O & d \end{bmatrix} \mathrm{SL}_n(F)$$

这便指明了:

推论 20

$$\mathrm{GL}_n(F) = D\mathrm{SL}_n(F)$$

其中 $D = \left\{ \begin{bmatrix} E_{n-1} & O \\ O & d \end{bmatrix} \middle| d \in F^* \right\}$

如下的矩阵生成的群的全体被称为初等群, 记作 E_n:

$$E_n = \{E_n + aE_{i,j} \mid i \neq j, a \in F\}$$

命题 21

$$E_n(F) = \mathrm{SL}_n(F)$$

Proof. $E_n(F) \subset \mathrm{SL}_n(F)$ 显然, 对于反向的包含式, 注意到 $\mathrm{SL}_n(F)$ 总可拆解为行列式为 1 的多个初等矩阵的积, 这些矩阵, 为不改变行列式的值, 应当包括:

(i) $E_n + kE_{i,j}$

(ii) 两次交换的积 $P_{i,j}P_{k,l}$

(iii) $P(ci)P(c^{-1}j)$

(i) 在 $E_n(F)$ 中是自然的, 对于 (ii), 不难知道 (i) 的复合只能实现将两行对换的同时其中一行取反, 按照下面的路径即可说明 (ii) 在 E_n 中:

$$i, j, k, l \to j, -i, k, l \to j, k, i, l \to j, k, l, -i \to j, i, l, k$$

对于 (iii), 注意如下的变换过程即可:

$$i, j \to i, j - ai \to i + a^{-1}j - i, j - ai \to a^{-1}j, j - ai \to a^{-1}j, -ai \to ai, a^{-1}j$$

□

命题 22

$$C_{\mathrm{SL}_n(F)} = \{(\delta_{i,j}a)_{n\times n} \mid a^n = 1\}$$

这命题探讨的只是何种矩阵总是交换的, 请读者回忆线性代数学中的知识自行补全证明.

命题 23 $\mathrm{SL}_n(F)$ 的换位子群为 $SL_n(F)$.

Proof. 证明 $E_n(F)$ 的换位子群为 $E_n(F)$ 即可, 为此查看下面的式子:

$$E + abE_{i,j} = (E + aE_{i,k})(E + bE_{k,j})(E - aE_{k,i})(E - bE_{i,k})$$

□

补充一些被我刻意略去的内容.
取定 $a, b \in G$, $aba^{-1}b^{-1}$ 被称为 G 的换位子, 换位子所生成的子群被称为 G 的换位子群, 记作 $[G, G]$.
Theorem 1 $[G, G] \lhd G, G/[G, G]$ 交换.
Proof. 只需证明 $\forall c \in [G, G], gcg^{-1}$, 考虑到 $gcg^{-1}c^{-1} \in [G, G]$, 自然 $gcg^{-1} \in [G, G]c = [G, G]$, 于是 $[G, G] \lhd G$.
取定 $x[G, G], y[G, G] \in G/[G, G]$, 注意到 $y^{-1}x^{-1}yx$ 作为换位子满足

$$[G, G] = y^{-1}x^{-1}yx[G, G]$$

必然存在

$$\begin{aligned} x[G, G]y[G, G] &= [G, G]xy[G, G] \\ &= [G, G]xyy^{-1}x^{-1}yx[G, G] = [G, G]yx[G, G] \\ &= y[G, G]x[G, G] \end{aligned}$$

至此证明完备. □

命题 24 若 $N < \mathrm{GL}_n(F)$ 在 $\mathrm{SL}_n(F)$ 的共轭作用下不变, 当其包含着非平凡初等矩阵时, $\mathrm{SL}_n(F) < H$.

Proof. 考虑 $n \geq 3$ 的情形, 不失一般性地假定是 $e_{1,2}^a = E + aE_{i,j}$ 在 N 中, 以 $P(a^{-1}b1)P(ab^{-1}3)$ 共轭作用于 e_{12}^a 上, 得到 e_{12}^b, 另外的, 注意到 $e_{1,j}^b = [e_{1,2}^b, e_{2,j}^1]$, 于是 $e_{1,j}^b$ 总在 N 中, 同样的针对 $e_{i,j}^b$ 使用等式 ${}_{i,j}^{b} = [e_{i,1}^1, e_{i,j}^b]$, 命题得到了证明.

恶俗小方框时间! 补充一下懒得在正文写的东西.
记法 $[a, b]$ 其实是换位子群的那个换位子, 也就是 $aba^{-1}b^{-1}$, 而对于 $\mathrm{SL}_{n>2}$ 的情形, 有下面的结论成立:

$$[e_{i,k}^a, e_{k,j}^b] = e_{i,j}^{ab}$$

证明只是简单的计算工作, 不再过多赘述, 正式命题证明中, $(e_{1,2}^b)^{-1}$ 作为 $e_{1,2}^b$ 的逆元自然在 N 中, 再依据 N 的共轭不变性, $e_{2,j}^1(e_{1,2}^b)^{-1}(e_{2,j}^1)^{-1}$ 自然在 N 中, 从而整个换位子已经在 N 中.

对于 $n = 2$ 的情形, 假定 $e_{1,2}^a$ 在 N 中, 考虑到 N 的共轭不变性, 得到构造

$$\begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} 1 & ab^2 \\ 0 & 1 \end{bmatrix}$$

上述形式的矩阵在 N 中, 取定其中“b”为 $b, b+1$ 的情形, 计算得到:

$$\begin{bmatrix} 1 & a(b+1)^2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & ab^2 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2ab \\ 0 & 1 \end{bmatrix}$$

现在, 假若 $\mathrm{char}F \neq 2$, 我们能少一堆屁事[1], 只需要求 $b = a^{-1}c$, 而 c 将 F^* 遍历, 证明便已经宣告了结束.

一堆屁事来了, 现在假定 $\mathrm{char}F = 2$, 我们首先将视丹如绿地发现 $1 = -1$ 这一不幸的事实, 在确认这事实在特征为 2 的域中确实成立后, 我们将可以通过共轭不变性声明:

妈的, 这 $\mathfrak{B}$ 数学是一天都学不下去了.

啊, 打错了, 是这个:

$$e_{21}^{a^{-1}} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}^{-1}$$

如法炮制之前的方法, 我们又能在 N 中找到 $e_{2,1}^{a^{-1}b^2}, e_{2,1}^{a^{-1}b^{-2}}$, 从而我们还能在 N 中构造出

$$\begin{bmatrix} 1 & ab^2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a^{-1}b^{-2} & 1 \end{bmatrix} \begin{bmatrix} 0 & a \\ a^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a^{-1}b^2 & 1 \end{bmatrix} = \begin{bmatrix} b^2 & 0 \\ 0 & b^{-2} \end{bmatrix}$$

[1]什么? 你说不知道什么叫域的特征值? 关我什么事, 反正我知道, 因为我会百度.

其中 $\begin{bmatrix} 0 & a \\ a^{-1} & 0 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, 对 $\begin{bmatrix} b^2 & 0 \\ 0 & b^{-2} \end{bmatrix}$, 考虑其如下在 N 中的换位子:

$$\left[\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} b^2 & 0 \\ 0 & b^{-2} \end{bmatrix}\right] = \begin{bmatrix} 1 & b^5+b \\ 0 & 1 \end{bmatrix}$$

于是, $e_{1,2}^{b^5+b}$ 在 N 之中, 应用式子 $(b+1)^4 = b^4+1$, 对其采用 $\begin{bmatrix} (b+1)^2 & 0 \\ 0 & (b+1)^{-2} \end{bmatrix}$ 引导的共轭变换, 得到 $e_{1,2}^{b}$ 在 N 之中, 考虑到 b 的任意性, 证明的工作已经完成. □

定理 25 假定 $F \neq F_2, F_3$, 取定 $\mathrm{GL}_2(F)$ 的一个子群 N 在 $\mathrm{SL}_2(F)$ 的共轭作用下不变, 若 N 不含于 $C_{\mathrm{GL}_2(F)}$ 中, 则 $\mathrm{SL}_2(F) \subset N$.

Proof. Step 1: 证明 N 中存在形如 $\begin{bmatrix} 0 & b \\ c & d \end{bmatrix}$ 的元素.

取定 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in N - C_{\mathrm{GL}_2(F)}$, 则

$$\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a-b\lambda & * \\ * & * \end{bmatrix}$$

$$\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a+c\lambda & * \\ * & * \end{bmatrix}$$

若 $b \neq 0 (c \neq 0)$, 取定 $\lambda = b^{-1}a (\lambda = -ac^{-1})$ 即可, 对于两者均为 0 的情况, 矩阵变为 $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$, 命题的成立只需要下面的式子:

$$\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a & \lambda d - a\lambda \\ 0 & d \end{bmatrix}$$

One Step Closer: 证明若 $F \neq F_5$, N 中存在形如 $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ 的矩阵, 其中 $a \neq d$.

在 Step 1 的基础上, 能够在 N 中找到如下的贵物:

$$\left[\begin{bmatrix} 0 & b \\ c & d \end{bmatrix}^{-1}, \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}^{-1}\right] = \begin{bmatrix} \lambda^2 & * \\ 0 & \lambda^{-2} \end{bmatrix}$$

考虑到 $F \neq F_{2,3,5}$, 我们便能够大言不惭地取定 $\lambda^4 \neq 1$, 也即是 $\lambda^2 \neq \lambda^{-2}$, 这导向了命题的成立.

In the End: 证明 N 中含有 $e_{1,2}^{\lambda_0}$.

当 $F \neq F_5$ 时, 针对 One Step Closer 中的结果有

$$\left[\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\right] = \begin{bmatrix} 1 & \lambda(1-ad^{-1}) \\ 0 & 1 \end{bmatrix}$$

考虑到 $a \neq d$ 的假设在先, 只需要取定一个非负的 λ 即可使得 $\lambda(1-ad^{-1})$ 称为满足条件的 λ_0.

对于 F_5 上的情形, 查看 Step 1 处的矩阵, 若 $c=-b^{-1}$, 当然很好, 否则查看换位子 $\left[\begin{bmatrix}1&1\\0&1\end{bmatrix},\begin{bmatrix}0&b\\c&d\end{bmatrix}\right]$, 依照 (i) 的方法, 能够构造所需形式的矩阵.

若 $d=0$, 只需变换

$$\left[\begin{bmatrix}0&b\\c&d\end{bmatrix},\begin{bmatrix}2&0\\b^{-1}&2^{-1}\end{bmatrix}^{-1}\right]=\begin{bmatrix}0&2^{-1}b\\2^{-1}b^{-1}&-1\end{bmatrix}$$

我们就得到了形式相似而 $d\neq 0$ 的矩阵, 那么, 再来查看下面的式子:

$$\left[\begin{bmatrix}0&b\\-b^{-1}&d\end{bmatrix}^{-1},\begin{bmatrix}2&0\\0&2^{-1}\end{bmatrix}^{-1}\right]^2=\begin{bmatrix}1&-bd\\0&1\end{bmatrix}$$

这是证明所需要初等阵, 至此证明完备. □

引理 26 秩为 r 的 $n\times n$ 矩阵可由 $\mathrm{SL}_n(F)$ 中的元素相似变换为如下的形式:

$$\begin{bmatrix}u_1&\cdots&u_r&0&\cdots&0\end{bmatrix}^{\mathrm{T}}$$

其中 $u_1,\cdots,u_r$ 彼此线性无关.

Proof. 利用对换 P_{ij} 先将矩阵一个线性无关部分组调整至一处, 这些对换合成为 P 后, 我们便能写出:

$$PAP^{-1}=\begin{bmatrix}u_1&\cdots&u_r&\cdots&u_n\end{bmatrix}^{\mathrm{T}}$$

对于后 $n-r$ 个矢量, 有关系 $u_i=\sum\limits_{j=1}^{r}b_{i,j}u_j$, 这关系实际上也可写作:

$$PAP^{-1}=\begin{bmatrix}u_1\\\vdots\\u_n\end{bmatrix}=\begin{bmatrix}I_r&O\\B&I_{n-r}\end{bmatrix}\begin{bmatrix}u_1\\\vdots\\u_r\\0\\\vdots\\0\end{bmatrix}$$

现在, 再要求 $Q=\begin{bmatrix}I&O\\-B&I\end{bmatrix}P$, 即得

$$QAQ^{-1}=\begin{bmatrix}u_1&\cdots&u_r&0&\cdots&0\end{bmatrix}^{\mathrm{T}}$$

□

定理 27 取定 $\mathrm{GL}_{n\geq 3}(F)$ 的一个子群 N 在共轭作用下不变, 若 $N\not\subseteq C_{\mathrm{GL}_n(F)}$ 则 $N\supset \mathrm{SL}_n(F)$.

Proof. 证明 N 里有一个初等矩阵即可, 依照题设我们将能够找到一个 $A\in N$ 与 $e_{i,j}^{\lambda}$ 不交换, 也即 $Ae_{i,j}^{\lambda}\neq e_{i,j}^{\lambda}A$, 这实在很有意义, 为此我们记 $T=[e_{i,j}^{\lambda},A]$, 依照 $e_{i,j}^{\lambda}=E+\lambda E_{i,j}$ 的本质, 立即有 $T=I+S$, 其中, 由于 $r(AE_{i,j}A^{-1})=1$, 立即有 $r(S)\leq 2$, 依照上一

条引理, 立即可以将 S 改写为 $PSP^{-1}=\begin{bmatrix}U_{2\times n}\\ O_{n-2\times n}\end{bmatrix}$, 这便提醒着我们 N 中有 $PTP^{-1}=\begin{bmatrix}A_1 & B_1\\ O & I_{n-2}\end{bmatrix}$, 当 $A_1=I_2$, 且不多言, 非如此, 则是 N 中有

$$\left[\begin{bmatrix}A_1 & B_1\\ O & I\end{bmatrix},\begin{bmatrix}I & X\\ O & I\end{bmatrix}\right]=\begin{bmatrix}I & (A_1-I)X\\ O & I\end{bmatrix}$$

无论如何, 我们得到了一个形如 $\begin{bmatrix}I & C\\ O & I\end{bmatrix}$ 的矩阵, 应用与引理证明类似的伎俩, 我们能够取到 $Q_1\in \mathrm{SL}_2(F), Q_2\in \mathrm{SL}_{n-2}(F)$, 使得

$$Q_1CQ_2^1=\begin{bmatrix}\lambda & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\end{bmatrix},\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & \lambda & \cdots & 0\end{bmatrix}$$

而

$$\begin{bmatrix}Q_1 & O\\ O & Q_2\end{bmatrix}\begin{bmatrix}I_2 & C\\ O & I_{n-2}\end{bmatrix}\begin{bmatrix}Q_1 & O\\ O & Q_2\end{bmatrix}^{-1}=\begin{bmatrix}I_2 & Q_1CQ_2^{-1}\\ O & I_{n-2}\end{bmatrix}=R\in N$$

对于 $Q_1CQ_2^{-1}$, 为前者时命题已经成立, 为后者时, $[e_{1,2}^{-1},R]=e_{1,4}^{-\lambda}$, 命题也成立. □

定义 3 (射影一般线性群与射影特殊线性群)

$$\mathrm{PGL}(F)=\mathrm{GL}(F)/C_{\mathrm{GL}_n(F)},\mathrm{PSL}(F)=\mathrm{SL}(F)/C_{\mathrm{SL}_n(F)}$$

推论 28 从我们针对 $n=2$ 与 $n\geq 3$ 证明的两个相似的命题上, 我们能够发现 $\mathrm{PSL}(F)$ 为单群.

定理 29 在 $\mathrm{SL}_n(F)=\mathrm{GL}_{n\geq 2}(F),(F\neq F_2,F_3)$ 中, $[\mathrm{SL}_n(F),\mathrm{SL}_n(F)]=[\mathrm{GL}_n(F),\mathrm{GL}_n(F)]$

Proof. 对于第一个等号, 正向的包含是自然的, 对于反向的包含, 依照定理 25,27, 我们只需在 $[\mathrm{SL}_n(F),\mathrm{SL}_n(F)]$ 中找到非中心的元素即可, 这元素可验证即是 $\left[\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix},\begin{bmatrix}0 & 1\\ -1 & 1\end{bmatrix}\right]$.

对于第二个等式, 反向的包含是自然的, 对于正向的包含, 不难注意到 $\det[A,B]=\det A\det B\det A^{-1}\det B^{-1}=1$ 于是命题的成立不必多言. □

注 1 $\mathrm{SL}_2(F_3)=[\mathrm{GL}_2(F_3),\mathrm{GL}_2(F_3)]$

Proof. 首先能够在 $[\mathrm{GL}_2(F_3),\mathrm{GL}_2(F_3)]$ 中找到:

$$\left[\begin{bmatrix}1 & 0\\ 0 & \lambda\end{bmatrix}^{-1},\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}^{-1}\right]=\begin{bmatrix}1 & 1-\lambda\\ 0 & 1\end{bmatrix}$$

取定 λ 为 -1, 即找到 $\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$ 在 $[\mathrm{GL}_2(F_3),\mathrm{GL}_2(F_3)]$ 中, 同时还将得到:

$$\begin{bmatrix}1 & 0\\ 0 & 2\end{bmatrix}\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 2\end{bmatrix}^{-1}=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$$

至此我们能够确定等式的成立. □

在体 (除环, 反称域) 上取定反自同构 $*: x \to x^*$ 满足

$$(x^*)^* = x, (x-y)^* = x^* - y^*, (xy)^* = y^* x^*$$

这反自同构被称为一个对合, 对合 $*$ 还将导出 $M_n(F)$ 上的一个对合:

$$*: (a_{i,j})^* \to (a_{j,i}^*)$$

例 3 在幺正空间中, $\mathbb{C}$ 上的共轭便是一个对合, 这对合引导出的矩阵上的对合正是共轭矩阵 $A^\dagger$, 所对应的 ε 为 $\pm 1, i$.

定义 4 取定体 F 上的矩阵 $H = \begin{bmatrix} O & I_n \\ \varepsilon I_n & O \end{bmatrix}$, 将矩阵

$$U_{2n}^{\varepsilon}(F) = \{U \in \mathrm{GL}_{2n}(F) \mid UHU^* = H\}$$

称为 F 上的一个 $2n$ 阶幺正群.

其中, 对于 F 为域的情况, 取 $* = \mathrm{id}_F, \varepsilon = -1$, 所得的 $U_{2n}^{-1}(F)$ 被称为辛群, 记作 $\mathrm{Sp}_{2n}(F)$, 而外加 $\mathrm{char} F \neq 2$ 的情况下, 取定 $\varepsilon = 1$ 得到的 $U_{2n}^{1}(F)$ 被称为正交群, 记作 $O_{2n}(F)$.

后面的内容太鸡肋了就不写了, 老老实实看典型群的内容吧.

群表示

记线性空间 V 上全体可逆线性变换为 $\mathrm{GL}(V)$, 若 $\dim V = n < \infty$, 则 $\mathrm{GL}_n(F) \simeq \mathrm{GL}(V)$.

定义 5 取定群 G 在 V 上的一个作用, 这作用若是线性的, 则称 V 是一个 G 模, 将生成作用的群同态映射 $\rho: G \to \mathrm{GL}(V)$ 称为 G 的一个表示, $\dim V$ 称为表示的维度或次数, 若 ρ 是单的, 称其是忠实的.

例 4 $\rho: G \to \mathrm{GL}(V), g \to \mathrm{id}_V$ 被称为平凡表示, 其一般被记为 $\varepsilon: G \to \mathrm{GL}_1(F) = F^*, g \to 1$.

取定一个 G 集 S, 为域 F 指定一个 S 生成的自由向量空间 FS, 线性延拓 G 在 S 上的作用至 FS, 得到 G 模 FS, 其上的表示在以 $g \in G$ 为基时得到的矩阵均为置换矩阵, 称为 S 诱导的置换表示.

查看作为 G 集的 G, 作用方式为群乘法, 将 FG 中元素 k 形式地记为 $k = \sum_{g \in G} k_g g$, 则如下的置换表示被称为正则表示:

$$\mathrm{Reg}(g)x = \sum_{g \in G} k_g \mathrm{Reg}(g) g$$

取定以 S_3 集 $\{a, b, c\}$ 生成的自由向量空间 V, 在这向量空间上, 考虑 S_3 上置换的线性延拓, 由于在基 a, b, c 上的取值确定, 这延拓是唯一的, 从而我们为 S_3 中元素找到了矩阵表示, 求法以轮换 $g = (abc)$ 为例:

$$g(a) = 0a + 1b + 0c$$

$$g(b) = 0a + 0b + 1c$$

$$g(c) = 1a + 0b + 0c$$

于是得到了

$$g \to \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

定义 6 取定表示 $\rho : G \to \mathrm{GL}(V)$, 若存在 V 的子空间 W, 使得 $\forall g \in G, gW \subset W$, 称 $\rho\mid_W : G \to GL(W)$ 为 ρ 的一个子表示, W 为 V 的 G 子模.

另外的, 在商空间 V/W 上附加群作用 $g(v+W) = g(v) + W$, 称为商表示, 另外的, V/W 也被称为商模.

使得下图交换的线性映射 σ 被称为表示同态或 G 模同态:

$$\begin{tikzcd} V_1 \arrow[r, "\sigma"] \arrow[d, "\rho_1(g)"] & V_2 \arrow[d, "\rho_2(g)"] \\ V_1 \arrow[r, "\sigma"] & V_2 \end{tikzcd}$$

更进一步地我们便有表示同构, G 模同构的概念, 记作 $\rho_1 \simeq \rho_2, V_1 \simeq V_2$.

引理 30 取定 G 模同态 $\sigma : V_1 \to V_2$, 则 $\mathrm{Ker}\sigma, \mathrm{im}\sigma$ 分别为 V_1, V_2 的子模, 且有 $V_1/\mathrm{Ker}\sigma \simeq \mathrm{im}\sigma$.

Proof. 所需的 G 模同构只是 $v + \mathrm{Ker}\sigma \to \sigma(v)$. □

不难为 G 模 V 找到一个极大的子 G 模 $V^{(1)}$, 其上的表示为平凡表示, 找到这样的子 G 模只需要我们将那些在任意 $g \in G$ 下不变的 V 中成员聚集在一起, 换言之,

$$V^{(1)} = \{v \in V \mid \forall g \in G, g(v) = v\}$$

注意到将有限群 G 中所有对象乘以 g 的某个元素只是对 G 中对象进行了一次重排, 于是我们能够确定, 取 $z = \frac{1}{|G|}\sum_{g\in G}\rho(g)$, 将有:

$$\forall g \in G, \rho(g)z = z\rho(g) = z$$

特殊的, 即得 $z^2 = z$.

假若 $v \in V^{(1)}$, 立即知晓 $v = \frac{1}{|G|}\sum_{g\in G} g(v) = z(v)$, 而对于 $z(v)$, 有:

$$\forall g \in G, g[z(v)] = gz(v) = z(v)$$

于是我们确信 $z(V) = V^{(1)}$, 取定 $V^{(0)} = (\mathrm{id}_V - z)V = \{v - z(v) \mid v \in V\}$, 由于 $z^2 = z$, 立即有

$$V = V^{(0)} \oplus V^{(1)}$$

对于 $V^{(0)}$, 额外地知道 $\rho(g)[v - z(v)] = \rho(g)v - z[\rho(g)v] \in V^{(0)}$, 于是 $V^{(0)}$ 同样是 V 的子 G 模, 故而这是对表示的直和分解, 这也便最终导出如下的引理:

引理 31 取定域 F 的特征 $\mathrm{char}F \nmid |G|$, 取定其上一个表示 ρ, 其中线性空间以 F 为基底, 取 $z = \frac{1}{|G|}\sum_{g\in G}\rho(g)$, 生成线性空间 $V^{(1)} = \{z(v) \mid v \in V\}, V^{(0)} = \{v - z(y) \mid v \in V\}$, 则 $V^{(1)}$ 正是 V 的极大平凡 G 子模, 且有如下分解:

$$V = V^{(1)} \oplus V^{(0)}$$

其中 $z\mid_{V^{(1)}} = \mathrm{id}_{V^{(1)}}, z\mid_{V^{(0)}} = 0$.

鉴于我高等代数学得稀烂期末被崔宝打了 67 分的好成绩, 这里补充一下幂等矩阵的直和分解是如何达成的, 取定 $\boldsymbol{A} \in \mathrm{End}V$, 满足 $\boldsymbol{A}^2 = \boldsymbol{A}$. 欲证明 $\mathrm{im}A \oplus im(\mathrm{id}_V - \boldsymbol{A}) = V$, 只需要:

Step 1: $\dim \mathrm{im}\boldsymbol{A} + \dim \mathrm{im}(\mathrm{id}_V - \boldsymbol{V}) = \dim V$

考虑到 $\mathrm{im}f = \mathrm{rank}f$, 只需证明 $r(A) + r(E - A) = n$ 即可, 为此查看

$$r(A) + r(E-A) = r\begin{bmatrix} A & O \\ O & E-A \end{bmatrix} = r\begin{bmatrix} A & A \\ A & E \end{bmatrix} = r\begin{bmatrix} A-A^2 & A \\ O & E \end{bmatrix} = r(E) = n$$

Step 2: $\mathrm{im}\boldsymbol{A} \cap \mathrm{im}(\mathrm{id}_V - \boldsymbol{A})$

取定 $\boldsymbol{A}v_1 = v_2 - \boldsymbol{A}v_2$, 等式两边叠加 $\boldsymbol{A}$ 得到 $\boldsymbol{A}v_1 = \boldsymbol{A}v_2 - \boldsymbol{A}v_2 = 0$, 于是命题得证.

例 5 取定 $S = \{e_1, e_2, e_3\}$ 与 $F(\mathrm{char}F > 3)$, 生成自由向量空间 FS, 得到 S_3 的一个置换表示, 依照引理计算, 即得

$$z = \frac{1}{6}\sum_{s \in S_3} s$$

于是 $z(e_i) = \dfrac{e_1 + e_2 + e_3}{3}$, 这便意味着

$$V^{(1)} = \mathrm{span}_F\{e_1 + e_2 + e_3\}$$

同样的, 对于 $\mathrm{id}_V - z$, 有 $(\mathrm{id}_V - z)e_i = ee_j + e_k - 2e_i$, 从而

$$V^{(0)} = \mathrm{span}_F\{e_1 + e_2 - 2e_3, e_1 + e_3 - 2e_2\}$$

这便构成了表示 V 的直和分解: $\mathrm{span}_F\{e_1, e_2, e_3\} = \mathrm{span}_F\{e_1 + e_2 + e_3\} \oplus \mathrm{span}\{e_1 + e_2 - 2e_3, e_1 + e_3 - 2e_2\}$.

既约表示与完全可约表示

定义 7 群 G 的一个表示若只有 $0, V$ 为子表示, 称其是既约的, 否则称其是可约的, 可约表示 V 若能分解为多个既约子表示的直和 $\oplus_{i=1}^n V_i$, 称这分解为既约分解, 称这可约表示是完全可约的.

命题 32 Abel 群在 $\mathbb{C}$ 上线性空间的既约表示总是一次的.

Proof. 取定 G 上既约表示 ρ, 注意到 $\rho(x)\rho(y) = \rho(xy) = \rho(yx) = \rho(y)\rho(x)$, 于是这些线性变换彼此交换, 取定其公共的特征向量 v, 在 $\mathrm{span}\{v\}$ 上, 诸多 $\rho(x)$ 自然是封闭的, 于是我们确定 $\mathrm{span}\{v\}$ 为 V 的一个子表示, 然而考虑到我们已经要求了 (V, ρ) 为一个既约表示, 只能是 $V = \mathrm{span}\{v\}$, 于是命题成立. □

同样做一些补充, 对于交换的线性变换 A, B, 取定 A 的一个特征值为 λ 的向量 η, 得到下面的式子成立:

$$AB\eta = BA\eta = \lambda B\eta$$

这指示我们一件事, 在 A 的诸多特征空间 V_{λ_i} 为 B 的不变子空间, 取定这子空间里 B 的特征向量, 立即得到了 A, B 共同的特征向量.

Abel 群 G 上的既约表示总是一次的, 为此我们可将表示所需的同态 ρ 视为 G 到 $\mathrm{GL}_1(F)$, 也即 F^* 上的同态, 这便将 G 的诸多可约表示与 G 到 F^* 的诸多同态结合了起来.

引理 33 (Schur) 取定 G 为群, 其上存在既约表示 V_1, V_2, 两个既约表示间具有 G 模同态 φ, 则 φ 要么是 0, 要么是 G 模同构.

Proof. $\mathrm{Ker}\varphi, \mathrm{im}\varphi$ 分别为 V_1, V_2 的子表示, 注意到 V_1, V_2 的既约属性, 立即知道 $\mathrm{Ker}\varphi, \mathrm{im}\varphi$ 要么分别为 V_1, V_2, 要么其一或全部为 0.

若 $\mathrm{Ker} f = V$, $\varphi = 0$, 否则 $\mathrm{Ker} f = 0$, 于是 φ 是单的, 且 $\mathrm{im}\varphi \neq \{0\}$, 于是又有 $\mathrm{im}\varphi = V_2$, 故而 φ 是满的, 这便导致了证明的结束. □

推论 34 $\mathbb{C}$ 上既约表示 V 的自同态 φ 必然是纯量变换.

Proof. 取定 φ 的一个特征值 α 及相应的特征向量 v_0, 查看 $v \in \mathbb{C}v_0$, 对任意的 $g \in G$, 立即知道

$$\varphi[g(v)] = g[\varphi(v)] = \alpha g(v)$$

于是 $g(v) \in \mathbb{C}v_0$, 从而 $\mathbb{C}$ 为 V 的一个子表示, 考虑 V 的既约属性, 非零的 $\mathbb{C}v_0$ 便是 V 本身, 从而确定了 $\varphi = \alpha \mathrm{id}_V$, 证明结束. □

定理 35 (Maschke) 取定 $\mathrm{char} F \nmid |G|$, 则有限群 G 在 F 上的任意有限维线性表示 V 总是完全可约的.

Proof. 取定 V 的一个子表示 W, 取定 W 作为线性空间在 V 上的补空间 W', 于是我们有线性空间直和分解 $V = W \oplus W'$, 取定 V 在 W' 上的投影 π, 立即有 $\pi_{W'} = \mathrm{id}_{W'}, \pi_W = 0$, 定义映射

$$\varphi : V \to W, v \to \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gv)$$

现在来证明 φ 为 G 模同态:

$$\begin{aligned}\varphi(\mathfrak{g}v) &= \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(g\mathfrak{g}v)\\ &= \frac{1}{|G|}\sum_{g\in G} \mathfrak{g}(g\mathfrak{g})^{-1}\pi(g\mathfrak{g}v) = \mathfrak{g}\frac{1}{|G|}\sum_{g\in G}(g\mathfrak{g})^{-1}\pi(g\mathfrak{g}v)\\ &= \mathfrak{g}\varphi(v)\end{aligned}$$

另外的, 显然 $\forall w \in W, \varphi(w) = w$, 于是 $\varphi\mid_W = \mathrm{id}_W$, 自然 $\mathrm{Ker}\varphi$ 是 V 的一个子表示, 对于这子表示, 从前显然成立着 $W \cap \mathrm{Ker}\varphi = \{0\}$, 于是

$$V = W \oplus \mathrm{Ker}\varphi$$

若 W 可约, 取定 U 作为 W 的非零真 G 子模, 若 U 仍然可约, 重复上述步骤, 由于表示是有限的, 最终我们总能取到 $W = U \oplus U'$, 其中 U 是既约的, 在二次情况下命题显然成立的前提下, 应用数学归纳法, 我们便完成了命题的证明. □

定理 36 有限群 G 在域 F 上的有限维表示若总是完全可约的, 必然有 $\mathrm{cahr} F \nmid |G|$.

Proof. 假若 $\mathrm{char} F \mid |G|$, 而其上的表示总是完全可约的, 考虑 G 在域 F 上生成的自由向量空间 FG 上的正则表示 Reg, 这是一个完全可约的表示, 取定 $c = \sum_{g\in G} g$, 立即知道 $\forall x \in G$,

$$\mathrm{Reg}(x)c = c$$

于是 Fc 是 FG 的一个一次子表示, 取定其余子表示 $FG = Fc \oplus W$, 查看恒等元 1 关于这表示的分解

$$1 = \alpha c + w, \alpha \in F, w \in W$$

据此得到

$$\sum_{g\in G} g(1) = \sum_{g\in G} g(\alpha c + w)$$

也即

$$c = \alpha \sum_{g\in G} g(c) + \sum_{g\in G} g(w) = \alpha|G|c + \sum_{g\in G} g(w)$$

考虑到在 F 中 $|G| = 0$, 立即有 $c = \sum\limits_{g\in G} g(w) \in W$, 然而 Fc 与 W 构成直和, 这使得 $c = 0$, 这与 $g \in G$ 作为 FG 的基是矛盾的. □

几个生成表示的方法

直和

取定 G 的一组表示 (ρ_n, V_n), 取定向量空间直和 $V = \bigoplus\limits_{i=1}^{n} V_i$, V 中元素表为形式和 $\sum\limits_{i=1}^{n} v_i$ 时, 定义

$$g(v) = \sum_{i=1}^{n} g(v_i)$$

这样的表示被称为 (ρ_i, V_i) 的直和, 记作 $\left(\bigoplus\limits_{i=1}^{n} \rho_i, \bigoplus\limits_{i=1}^{n} V_i\right)$.

反轭表示

取定 G 的一个表示 (ρ, V), 取定 V 的对偶空间 V^*, 为 $f \in V^*, g \in G$ 指定线性泛函 $\rho^*(g)(f) : V \to F, v \to f(g^{-1}v)$, 于是 $\rho^*(g) : V^* \to V^*, f \to \rho^*(g)(f)$ 为 V^* 上的一个线性变换, 而指派 $\rho^* : g \to \rho^*(g)$ 便使得 V^* 成为一个搭载了群作用的线性空间, 再查看下面的式子:

$$\rho^*(1)(f)(v) = f(v) \Rightarrow \rho^*(1)(f) = f \Rightarrow \rho^*(1) = \mathrm{id}_{V^*}$$

$$\begin{aligned}[\rho^*(g_1)\rho^*(g_2)(f)](v) &= [\rho^*(g_2)]f(g_1^{-1}v) = f(g_2^{-1}g_1^{-1}v) \\ &= f[(g_1g_2)^{-1}v] = \rho(g_1g_2)(f)(v)\end{aligned}$$

于是 $\rho^*(g_1g_2) = \rho^*(g_1)\rho^*(g_2)$, 这便表明了 V^* 为一个 G 模, 称为反轭表示.

(这里本来还有一个表示的张量积的, 但是我已经被黎景辉的高等线性代数伤害过了, 就不写了, 等下学期学那本群与代数表示的时候再说吧, 顺带整合下李克正、蓝以中等书上的材料写个多重线性代数的 DLC 出来.)

表示的提升

依靠群同态 $f : G_1 \to G_2$ 与表示 $\rho : G_2 \to \mathrm{GL}(V)$, 立即可通过复合 $f\rho : G_1 \to \mathrm{GL}(V)$ 得到 G_1 的一个表示, 称这表示是 ρ 通过 f 的提升.

例 6 取定 $H < G$, $\iota : H \to G$ 为嵌入映射, 若 G 具有表示 $\rho : G \to V$, 立即得到 H 上表示 $\rho\iota$, 这是 ρ 在 H 上的限制, 记为 $\mathrm{Res}_H^G V$.

取定 $H \lhd G$, 查看下面的交换图表:

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, "\pi"'] & \mathrm{GL}(V) \\ G/H \arrow[ur, "\bar{\rho}"'] & \end{tikzcd}$$

其中 π 为自然同态, 对于表示 $\bar{\rho}$, 立即可以通过提升得到 G 的表示 $\rho = \bar{\rho} \circ \pi$, 其中不难发现 $\mathrm{Ker}\rho \supset H$, 另外的, 对于表示 ρ, 假若 $H \subset \mathrm{Ker}\rho$, 依照商群所具有的泛性质, 立即知道了使得图表交换的同态 $\bar{\rho}$ 的存在性.

现在我们在如下的两个对象间建立了一一对应的关系:

$$G \text{ 上满足 } H \subset Ker\rho \text{ 的表示 } \rho$$
$$G/H \text{ 上的表示}$$

诱导表示

取定群 G 的表示 (ρ, V), 以及其上的一个子群 H, 在 V 中取定 H 不变的子表示 W, 这子表示同时也是 $\mathrm{Res}_H^G V$ 的子表示. 为 $g \in G$ 指定 $gW = \{g(w) \mid w \in W\}$, 自然这是线性空间 V 的一个子空间, 考虑到 $hW \subset W$, 当 $g_1 H = g_2 H$ 时, 有 $g_1 = g_2 h_2$ 与 $g_2 = g_1 h_1$, 从而得到 $g_2 W \subset g_1 W, g_1 W \subset g_2 W$, 于是下面的记法是合理的:

$$\sigma H = gH, g \in \sigma = G/H$$

假若 V 能够被表为

$$V = \bigoplus_{\sigma \in G/H} \sigma W$$

则称 V 是 W 的诱导表示, 记作 $\mathrm{Ind}_G^G W$.

例 7 取定 $H < G$, 考虑 G 的正则表示 $\mathrm{span}_F G$ 与 H 的正则表示 $\mathrm{span}_F H$, 自然 $\mathrm{span}_F H$ 是 $\mathrm{Res}_H^G V$ 的子空间, 另外的, 考虑到 $h\mathrm{span}_F H = \mathrm{span}_F hH = \mathrm{span}_F H$, 于是 $\mathrm{span}_F H$ 是 H 不变的, 立即知道 $\mathrm{span}_F H$ 是 $\mathrm{Res}_H^G V$ 的 H 子模, 取定 H 的两个陪集 $g_1 H, g_2 H$, 取定 $g_1(w_1) = g_2(w_2)$, 立即得到等式

$$\sum_{h \in H} k_h g_1 h = \sum_{h \in H} k'_h g_2 h$$

也即 $\displaystyle\sum_{x \in g_1 H} k_x x = \sum_{y \in g_2 H} k_y y$, 考虑到不同陪集正是线性无关向量组, 从而能够确定 $g_1 W \cap g_2 W = \{0\}$, 另外的, 从 $G = \displaystyle\bigcup_{g \in G} gH$, 便能确定

$$\bigoplus_{\sigma \in G/H} \sigma \mathrm{span}_F H = \mathrm{span}_F G$$

也即是 $\mathrm{span}_F G = \mathrm{Ind}_H^G$.

特征标

定义 8 取定群 G 的一个表示 (V,ρ), 为 $\rho(g)$ 指定线性函数 $\chi_\rho : G \to F, g \to \mathrm{tr}\rho(g)$, 这线性函数被称为表示的一个特征标, 也称为 G 的一个特征标, 同样的, 若 ρ 既约, 称 χ_ρ 是既约特征标, 另外的, 若 (ρ, V) 是一次表示, 称 χ_ρ 为线性特征标.

例 8 取定 S_3 的置换表示, 立即有:

$$\chi_\rho[(1)] = \mathrm{tr}\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} = 3, \chi_\rho[(12)] = \mathrm{tr}\begin{bmatrix}0&1&0\\0&0&1\\0&0&1\end{bmatrix} = 1, \chi_\rho[(123)] = \mathrm{tr}\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix} = 0$$

命题 37 取定 G 的两个 F 表示 $(\rho, V), (\rho_1, V_1), (\rho_2, V_2)$, 则

(i) $\rho_1 \simeq \rho_2$, 则 $\chi_{\rho_1} = \chi_{\rho_2}$.

Proof. 回忆我们对 G 模同构的定义, 知道式子 $\sigma\rho_1(g) = \rho_2(g)\sigma$ 的成立, 于是

$$\sigma\rho_1(g)\sigma^{-1} = \rho_2(g)$$

知道矩阵的秩是相似不变量, 于是 $\mathrm{tr}\sigma(g) = \mathrm{tr}\sigma(g)$ 总是成立的, 这便是 $\chi_{\rho_1} = \chi_{\rho_2}$. □

(ii) 若 $g, h \in G$ 共轭, 则 $\chi_\rho(g) = \chi_\rho(h)$, 也即同一共轭类中的元素特征标一致.

Proof. 证明显然, 再问自杀. □

(iii) 取定 λ, χ 是 G 的一个线性特征标与既约特征标, 则 $\lambda \circ \chi$ 是 G 的既约特征标.

Proof. 捏妈妈的证明要用张量积. □

(iv) $\chi_{\rho^*}(g) = \chi_\rho(g^{-1})$

Proof. 注意到

$$\rho^*(g)(v_p^*)(g \cdot v_q) = v_p^*(g^{-1}g \cdot v_q) = v_p^*(v_q) = \delta_{p,q}$$

取定 $\rho^*(g), \rho(g)$ 的矩阵分别为 $(t_{p,i})_{n\times n}, (k_{q,j})_{n\times n}$, 于是

$$\begin{aligned}\left(\sum_{i=1}^n t_{p,i}v_i^*\right)\left(\sum_{j=1}^n k_{q,j}v_j\right) &= \sum_{i=1}^n t_{p,i}v_i^*\left(\sum_{j=1}^n k_{q,j}v_j\right)\\ &= \sum_{i,j=1}^n t_{p,i}k_{q,j}\delta_{i,j}\\ &= \sum_{l=1}^n t_{p,l}k_{q,l} = \delta_{p,q}\end{aligned}$$

这 TM 意味着什么? 这 TM 意味着 $(t_{p,i})_{n\times n}(k_{q,j})^{\mathrm{T}}_{n\times n} = E_n$, 命题至此若再不成立, 请小心我半夜来你家上吊. □

(v) 若 W 为 V 的子表示, $\chi_{\rho_V} = \chi_{\rho_W} + \chi_{\rho_{V/W}}$.

Proof. 自然有 $V = W \oplus W', W' \simeq V/W$, 于是首先有 $\mathrm{tr}\rho_V(g) = \mathrm{tr}\rho_W(g) + \mathrm{tr}\rho_{W'}(g)$, 另外的, 若 W' 具有基 $\{w'_n\}$, V/W 自然具有基 $\{w'_n + W\}$, 考虑到 W 是 G 不变的, 于是

$$g \cdot (w'_n + W) = g \cdot w'_n + W$$

从而我们还有 $\mathrm{tr}\rho_{V/W}(g) = \mathrm{tr}\rho_{W'}(g)$, 结合前面的式子, 等式已经成立. □

记表示 $\rho : H \to \mathrm{GL}(W)$ 在 G 上的诱导表示为 $(\rho^G, \mathrm{Ind}_H^G W)$, 其特征标为 χ^G, 注意到诱导表示 $\mathrm{Ind}_H^G W$ 上 g 将 $g_0 HW$ 作用为 $(gg_0)HW$, 取定诸多 G 不变的子空间 $\sigma W, \sigma \in G/H$ 生成 $\mathrm{Ind}_H^G W$ 的直和分解, 于是可以按照下面的手段计算 $\rho^G(g)$ 的迹:

$$\chi^G(g) = \mathrm{tr}\rho^G(g) = \sum_{\sigma} \mathrm{tr}\rho^G \mid_{\sigma W}$$

针对 $\mathrm{tr}\rho^G \mid_{\sigma W}$ 额外地从 $g\sigma = \sigma$ 中推知 $g_0 g g_0^{-1} \in H, g_0 \in \sigma$, 于是 $\forall w \in W, g(g_0 w) = (g_0 g_0^{-1}) g(g_0 w) = g_0(g_0^{-1} g g_0) w$, 这便意味着 $g(\sigma W) = \sigma(g_0^{-1} g g_0 W)$, 依照交换图

$$\begin{tikzcd} W \arrow[r, dash, "\sigma"] \arrow[d, "g_0^{-1} g g_0"'] & \sigma W \arrow[d, "g"] \\ W \arrow[r, dash, "\sigma"] & \sigma W \end{tikzcd}$$

立刻知道

$$\mathrm{tr}\rho(g) \mid_{\sigma W} = \mathrm{tr}_W \rho(g_0^{-1} g g_0) = \chi_W(g_0 g g_0)$$

从而 $\chi^G(g) = \sum_{\sigma} \chi_W(g_0^{-1} g g_0)$, 注意到针对任意的 $x \in \sigma$ 总有 $x = g_0 h$, 于是 $x^{-1} g x = h^{-1}(g_0^{-1} g g_0) h$, 考虑到特征标的共轭不变性, 得到

$$\chi_W(g_0^{-1} g g_0) = \chi_W(x^{-1} g x)$$

这其中不同的 x 共有 $|\sigma| = |H|$ 个, 综上即得

定理 38

$$\chi^G(g) = \sum_{\sigma} \chi_W(g_0^{-1} g g_0)$$

特殊的, $\mathrm{char} F \nmid |H|$ 时,

$$\chi^G(g) = \frac{1}{|H|} \sum_{x^{-1} g x \in H} \chi_W(x^{-1} g x)$$

例 9 查看 $S_3 < S_4$, 依照例 5, 在 $V^{(0)}$ 上有

$$\chi(1) = \mathrm{tr} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 2$$

$$\chi(12) = \mathrm{tr} \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix} = 0, \chi(13) = \mathrm{tr} \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} = 0, \chi(12) = \mathrm{tr} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = 0$$

$$\chi(123) = \mathrm{tr} \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} = -1$$

于是在 $\mathrm{Ind}_{S_3}^{S_4}V^{(0)}$ 上, 有

$$\chi^G(1)=\frac{1}{|S_3|}\sum_{x^{-1}(1)x\in S_3}\chi[x^{-1}(1)x]=\frac{|S_4|}{|S_3|}\chi(1)=8$$

$$\chi^G(132)=\frac{1}{|S_3|}\sum_{x^{-1}(132)x\in S_3}\chi[x^{-1}(1)x]=\frac{|S_3|}{|S_3|}\chi(123)=-1$$

引理 39 取定 $\mathbb{C}$ 上群 G 的两个既约表示 V_1,V_2, 其上有 G 模同态 $\varphi:V_1\to V_2$, 取定

$$\zeta=\frac{1}{|G|}\sum_{g\in G}\rho_2(g)^{-1}\varphi\rho_1(g)$$

若 ρ_1 与 ρ_2 不同构, $\zeta=0$, 若 $V_1=V_2,\rho_1=\rho_2$, 则 $\zeta=\dfrac{\mathrm{tr}\varphi}{\dim V}\mathrm{id}_V$.

Proof. 任取 $g'\in G$, 有

$$\rho_2(g)^{-1}\zeta\rho_1(g')=\frac{1}{|G|}\sum_{g\in G}\rho_2(gg')^{-1}\varphi\rho_1(gg')=\zeta$$

即得 $\zeta\rho_1(g')=\rho_2(g')\zeta$, 于是 ζ 同样是一个 G 模同态, 现在利用 Schur 引理 (引理 33), 若是前一种情况, $\varphi=0$, 于是 $\zeta=0$, 若是后一种情况 ζ 为一纯量变换, 又 $\rho_1=\rho_2$ 时 $\mathrm{tr}\zeta=\mathrm{tr}\dfrac{1}{|G|}\sum\limits_{g\in G}\rho(g)^{-1}\varphi\rho(g)=\dfrac{1}{|G|}\sum\limits_{g\in G}\mathrm{tr}\rho(g)^{-1}\varphi\rho(g)=\dfrac{|G|}{|G|}\mathrm{tr}\varphi$, 于是为了使得这等式成立, 必须

$$\xi=\frac{\mathrm{tr}\varphi}{\dim V}\mathrm{id}_V$$

□

现在将 $\rho_1(g),\rho_2(g)$ 改写为矩阵的形式:

$$\rho_1(g)=(a_{i_1,j_1}(g))_{n\times n},\rho_2(g)=(a_{i_2,j_2}(g))_{n\times n}$$

同样的将 G 模同态 φ,ζ 写作 $(x_{i_2,i_1})_{n\times n},(x'_{i_2,i_1})_{n\times n}$, 依照 ζ 的定义式立即有

$$x'_{i_2,i_1}=\frac{1}{|G|}\sum_{g,j_{1,2}}a_{i_2,j_2}(g^{-1})x_{j_2,j_1}a_{i_1,j_1}(g)$$

假若 ρ_1,ρ_2 不同构, $\zeta=0$, 于是针对任意的 x_{j_2,j_1} 均成立 $x'_{i_2,i_1}=\dfrac{1}{|G|}\sum\limits_{g,j_{1,2}}a_{i_2,j_2}(g^{-1})x_{j_2,j_1}a_{i_1,j_1}(g)=0$, 另外的, 假若 $\rho_1=\rho_2,\zeta$ 同时也便可写为 $\dfrac{\mathrm{tr}\varphi}{\dim V}\mathrm{id}_V$, 于是有

$$\frac{1}{|G|}\sum_{g,j_1,j_2}a_{i_2,j_2}(g^{-1})x_{j_2,j_1}a_{j_1,i_1}(g)=\frac{1}{n}\sum_{j_1,j_2}\delta_{i_2,i_1}\delta_{j_2,j_1}x_{j_2,j_1}$$

比较系数立即得到

推论 40 ρ_1,ρ_2 不同构时针对任意的 $i_{1,2},j_{1,2}$ 均成立

$$\frac{1}{|G|}\sum_{g\in G}a_{i_2,j_2}(g^{-1})a_{j_1,i_1}(g)=0$$

$\rho_1=\rho_2$ 时

$$\frac{1}{|G|}\sum_{g\in G}a_{i_2,j_2}(g^{-1})a_{j_1,i_1}(g)=0$$

取定关于 G 上 F 值函数 φ,ψ, 生成相应的内积为 $(\varphi,\psi)=\dfrac{1}{|G|}\sum_{g\in G}\varphi(g^{-1})\varphi(g)$ 对于 G 的两个表示 $(V_1,\rho_1),(V_2,\rho_2)$ 同样的取定特征标的内积, 当 ρ_1,ρ_2 不同构时自然有 $(\chi_{\rho_1},\chi_{\rho_2})=0$.

取定 F 为 $\mathbb{C}$, 对于其上的既约表示 (V,ρ), 将 $\rho(g)$ 写为矩阵形式 $(a_{i,j}(g))_{n\times n}$, 于是 $\chi(g)=\sum_{i=1}^{n}a_{i,i}(g)$, 故而

$$(\chi,\chi)=\sum_{g\in G}\sum_{i,j=1}^{n}a_{i,i}(g^{-1})a_{j,j}(g)$$

另外的, 依照推论 40, 有 $\sum_{i,j=1}^{n}a_{i,i}(g^{-1})a_{j,j}(g)=\dfrac{\delta_{i,j}}{n}$, 从而 $(\chi,\chi)=\dfrac{1}{n}\sum_{i,j=1}^{n}\delta_{i,j}=1$.

综上我们有

定理 41 (特征标的正交) 取定 $\mathrm{char}F\nmid|G|$, G 上有既约表示 V_1,V_2, 当 ρ_1,ρ_2 不同构时, $(\chi_1,\chi_2)=0$, 若 ρ_1,ρ_2 同构, $(\chi_1,\chi_2)=1$.

定理 42 取定 $\mathbb{C}$ 上群 G 表示 (ρ,V), 其有如下的既约分解:

$$V=\bigoplus_{i=1}^{m}n_iV_i$$

假若 V,V_i 的特征标为 χ,χ_i, 则 $n_i=(\chi,\chi_i)$, 称为 V_i 的重数.

Proof. 立即知道 $\chi=\sum_{i=1}^{m}n_i\chi_i$, 于是

$$(\chi,\chi_i)=\sum_{j=1}^{r}n_i(\chi_i,\chi_j)=n_i$$

□

推论 43 考虑到重数直接由各个既约子表示于 V 本身确定, $\mathbb{C}$ 上表示 V 的既约分解是唯一的.

推论 44 $\mathbb{C}$ 上表示同构当且仅当其特征标全同.

Proof. 正向命题显然, 反向命题只需注意到针对任意的既约表示 λ 总有 $(\chi_1,\chi_\lambda)=(\chi_2,\chi_\lambda)$. [1] □

推论 45 $\mathbb{C}$ 上表示 V 既约当且仅当 $(\chi,\chi)=1$.

Proof. 正向命题显然, 对于反向论述, 反设不成立, 只来看如下两个基本情况:

$$V=2V_0,V=V_1\oplus V_2$$

两种情况分别导致了

$$(\chi_\rho,\chi_\rho)=2^2(\chi_{\rho_0},\chi_{\rho_0})=4,(\chi_\rho,\chi_\rho)=(\chi_{\rho_1},\chi_{\rho_1})+2(\chi_{\rho_1},\chi_{\rho_2})+(\chi_{\rho_2},\chi_{\rho_2})=2$$

这自然导致了矛盾, 其余情况与此类似, 于是命题成立. □

[1]我知道这段证明槽点不少, 但是这本天杀的教材都没证明既约分解的唯一性, 就别强求我了, 不然我来你家上吊吧.

例 10 取定有限群 G 上正则表示 Reg, 立即知道 $\mathrm{Reg}g(g') = gg'$, 而 $gg' = g'$ 当且仅当 $g = 1$, 这意味着非 1 的 $\mathrm{Reg}(g)$ 的对角线上元素必定为 0, 从而迹为 0, 同样的, 对于 $\mathrm{Reg}(1) = \mathrm{id}_V$, 迹立即为 $|G|$, 故而有

$$\chi(g) = \begin{cases} |G|, g = 1 \\ 0, g \neq 1 \end{cases}$$

推论 46 有限群 G 的既约复表示总同构于 G 的正则表示的既约分解中的一个直和项, 且该直和项的重数于该表示的次数一致.

Proof. 注意查看下面的式子即可:

$$(\chi, \chi_i) = \frac{1}{|G|} \sum -g \in G\chi(g^{-1})\chi_i(g) = \frac{|G|}{|G|}\chi_i(1) = n_i$$

□

推论 47 有限群 G 复表示的各个既约表示次数 n_i 满足

$$\sum_{i=1}^{m} n_i^2 = \sum_{i=1}^{m} n_i\chi_i(1) = \chi(1) = |G|$$

另外的,

$$\forall g \neq 1, \sum_{i=1}^{m} n_i\chi_(g) = \chi(g) = 0$$

知道诸多特征标在共轭类上取值一致, 于是特征标可以看作是共轭类的函数, 取定 G 上共轭类函数的全体为 K, 知道 G 诸多既约表示的特征标是一组标准正交向量, 另外的, 假定 $f \in K$ 与全体既约特征标 χ_i 正交, 取定辅助映射

$$\varphi_f = \sum_{g \in G} f(g)\rho(g)$$

考虑到

$$\rho(g_1^{-1})\varphi_f\rho(g_1) = \sum_{g \in G} f(g)\varphi(g_1^{-1}gg_1) = \sum_{g \in G} f(g)\varphi(g) = \varphi_f$$

从而 $\rho(g_1)\varphi_f = \varphi_f\rho(g_1)$, 依照 Schur 引理 (引理 33)$\varphi$ 为一纯量变换, 考虑到 f 与 χ_i 的正交关系, 立即确定 $\mathrm{tr}\varphi_f = 0$, 从而 $\varphi_f = 0$, 从而

$$0 = \varphi_f(1) = \sum_{g \in G} f(g)\rho(g)(1) = \sum_{g \in G} f(g)(g)$$

考虑到 g 彼此线性无关, 于是 $\forall g \in G, f(g) = 0$.

另外的, 群 G 总可分解为共轭类的不交并, 故而假若群 G 有 r 个共轭类, 由于以此能够给共轭类的对偶空间取定一组对偶基, 于是作为正交向量基的 χ_i 成为 r 个典型基向量.

于是我们有如下结论:

定理 48 G 上复表示的既约特征标组成 G 上类函数空间里的标准正交基, 另外的, G 中的既约表示数目与 G 的共轭类数目一致.

例 11 取定 $G=\langle a,b\rangle \simeq \mathbb{Z}_2\times\mathbb{Z}_2$, 这群自然交换, 于是从前, 这群的既约表示均是一维的, 考虑到 $4=\sum_{i=1}^{4} n_i^2$, 于是很容易得到如下的特征标标 (第一、二行分别是共轭类的代表元)

	1	1	1	1
	1	a	b	ab
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1