

# 群论笔记 Chapter 2: 有限阿贝尔群结构与群的构建

群论课程笔记

2025 年 12 月 2 日

## 目录

<b>1 群的构建：直积与直和</b>	<b>2</b>
1.1 定义	2
1.2 中国剩余定理 (CRT) 的群论形式	2
1.3 中国剩余定理 (CRT) 的群论证明	2
<b>2 有限阿贝尔群的结构定理</b>	<b>4</b>
2.1 不变因子分解	4
<b>3 结构定理的证明：初级分解</b>	<b>4</b>
<b>4 结构定理的证明：从初等因子到不变因子</b>	<b>6</b>
4.1 算法目标	6
4.2 重组算法 (Recombination Algorithm)	6
4.3 整除性的验证	7
<b>5 商群构建：正规子群与商群 (笔记 P2-P4)</b>	<b>7</b>
5.1 为什么要引入“正规子群”?	8

5.2	商群的定义与例子	8
6	商群的严格证明与第一同构定理基础 (笔记 P6, P7)	8
6.1	运算良定性的详细证明	9
6.2	核与正规子群的关系	9
6.3	经典同构关系	9
7	第一同构定理：泛性质与同构 (笔记 P8, P9)	9
7.1	诱导同态的存在性 (泛性质)	10
7.2	第一同构定理	10
7.3	第一同构定理的详细证明	10
8	约化映射 (Reduction Map) (笔记 P12)	11
8.1	整数模 $n$ 到模 $d$ 的映射	12
8.2	一般化推广	12
9	换位子、导群与特征子群 (笔记 P13, P14)	12
9.1	换位子与导群	12
9.2	经典导群例子的详细证明	12
9.3	特征子群 (Characteristic Subgroup)	14
9.4	重要性质与证明	14
9.5	特征子群性质的详细证明	14
10	群的直积与泛性质 (笔记 P16, P20)	16
10.1	外直积 (External Direct Product) —— 组装	16
10.2	内直积 (Internal Direct Product) —— 拆解判据	16
10.3	泛性质 (Universal Property)	17

<b>11 矩阵群与短正合列 (Matrix Groups)</b>	<b>18</b>
11.1 补充：短正合列详解与实例分析	18
11.1.1 短正合列的形式化定义	19
11.1.2 矩阵群序列的具体分析	19
<b>12 半直积 (Semi-direct Product)</b>	<b>20</b>
12.1 外半直积 (构造篇)	21
12.2 内半直积 (识别篇)	22
12.3 实例详解： $S_4$ 的分解	22
<b>13 同构定理的详细证明 (Isomorphism Theorems)</b>	<b>23</b>
13.1 第三同构定理 (The Third Isomorphism Theorem)	24
13.2 第二同构定理 (The Second Isomorphism Theorem)	24
<b>14 有限群的分类 (Classification)</b>	<b>26</b>
14.1 六阶群的分类	26
14.2 八阶群的分类	26
<b>15 可解群 (Solvable Groups)</b>	<b>26</b>
15.1 背景：伽罗瓦理论	27
15.2 定义：导子列与可解性	27
15.3 基本性质与例子	27
15.4 实例详解：上三角矩阵群 $T_n(k)$	30
15.4.1 定义与符号	30
15.4.2 证明：利用正规列证明可解性	31
15.4.3 另一种视角：导子列的指数级收缩	32
15.4.4 具体例子： $n = 3$ 的情形	32

<b>16 幂零群 (Nilpotent Groups)</b>	<b>33</b>
16.1 定义：下中心列 . . . . .	33
16.2 等价定义：上中心列 . . . . .	34
16.3 性质与反例 . . . . .	36
<b>17 特征子群 (Characteristic Subgroups)</b>	<b>40</b>
<b>18 单群 (Simple Groups)</b>	<b>40</b>
18.1 定义 . . . . .	40
18.2 分类 . . . . .	40
<b>19 总结对比</b>	<b>41</b>
19.1 核心实例：证明 $PSL_2(k)$ 是单群 . . . . .	41

## 本章导读

1. 有限阿贝尔群结构定理：引入直积与直和，详述结构定理的两种形式（初等因子与不变因子），并给出了初级分解的详细证明。

# 1 群的构建：直积与直和

## 1.1 定义

定义 1.1 (直积 External Direct Product). 给定群  $G_1, \dots, G_n$ , 其直积定义为集合  $G_1 \times \dots \times G_n$  配上分量运算:

$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$$

定义 1.2 (直和 Internal Direct Sum). 设  $G$  是加法群,  $H_1, \dots, H_n$  是其子群。若  $G$  中任一元素  $x$  可唯一表示为  $x = x_1 + \dots + x_n$  ( $x_i \in H_i$ ), 则称  $G$  为这些子群的直和, 记作:

$$G = H_1 \oplus \dots \oplus H_n$$

## 1.2 中国剩余定理 (CRT) 的群论形式

对于有限循环群, 我们有以下重要同构判据:

命题 1.3.

$$C_a \oplus C_b \cong C_{ab} \iff \gcd(a, b) = 1$$

## 1.3 中国剩余定理 (CRT) 的群论证明

命题 1.4 (CRT 的群论形式). 设  $C_m, C_n$  分别为  $m$  阶和  $n$  阶循环群。则:

$$C_m \times C_n \cong C_{mn} \iff \gcd(m, n) = 1$$

证明. 记  $C_m = \langle a \rangle$  且  $|a| = m$ ,  $C_n = \langle b \rangle$  且  $|b| = n$ 。直积群  $G = C_m \times C_n$  的阶为  $|G| = mn$ 。我们需要证明  $G$  是循环群当且仅当  $\gcd(m, n) = 1$ 。

1. 充分性 ( $\Leftarrow$ ) 假设  $\gcd(m, n) = 1$ 。考虑元素  $g = (a, b) \in G$ 。我们需要计算  $g$  的阶  $|g|$ 。设  $k$  为使  $g^k = (a^k, b^k) = (e_m, e_n)$  的最小正整数。

- $a^k = e_m \implies m \mid k$ 。

- $b^k = e_n \implies n \mid k$ 。

因此,  $k$  必须是  $m$  和  $n$  的公倍数。根据阶的定义,  $k$  应为最小公倍数:

$$|g| = \text{lcm}(m, n)$$

由于  $\gcd(m, n) = 1$ , 我们要用到数论性质  $\text{lcm}(m, n) \cdot \gcd(m, n) = mn$ 。故  $|g| = \text{lcm}(m, n) = mn$ 。因为群  $G$  的大小为  $mn$ , 且我们找到了一个阶为  $mn$  的元素  $g$ , 所以  $G$  是由  $g$  生成的循环群。即  $G \cong C_{mn}$ 。

**2. 必要性 ( $\implies$ )** 假设  $\gcd(m, n) = d > 1$ 。我们要证明  $G$  不是循环群。对于  $G$  中的任意元素  $x = (a^i, b^j)$ , 计算其阶的最大可能值。

$$x^{\text{lcm}(m, n)} = ((a^i)^{\text{lcm}(m, n)}, (b^j)^{\text{lcm}(m, n)})$$

由于  $m \mid \text{lcm}(m, n)$  且  $n \mid \text{lcm}(m, n)$ , 所以  $a^{\text{lcm}(m, n)} = e_m$  且  $b^{\text{lcm}(m, n)} = e_n$ 。这意味着对于任意  $x \in G$ , 其阶都整除  $\text{lcm}(m, n)$ 。但是:

$$\text{lcm}(m, n) = \frac{mn}{\gcd(m, n)} = \frac{mn}{d} < mn$$

也就是说,  $G$  中所有元素的阶都严格小于群的阶  $mn$ 。不存在阶为  $mn$  的生成元, 因此  $G$  不是循环群。□

### 直观理解: 直观理解: 赛跑模型

想象两个人在跑道上跑步。

- A 跑一圈用  $m$  分钟, B 跑一圈用  $n$  分钟。
- 他们同时出发, 问多久后两人同时回到起点?
- 答案是  $\text{lcm}(m, n)$ 。
- 如果  $m, n$  互质 (比如 4 和 3), 他们要在跑了  $4 \times 3 = 12$  分钟后才重逢 (遍历了所有可能的相位组合)。
- 如果  $m, n$  不互质 (比如 4 和 6), 他们在 12 分钟就重逢了, 而不是 24 分钟。这意味着有些状态组合永远达不到。

## 2 有限阿贝尔群的结构定理

### 2.1 不变因子分解

**定理 2.1** (有限阿贝尔群基本定理 - 不变因子形式). 任何有限阿贝尔群  $G$  都可以唯一地分解为循环群的直和:

$$G \cong C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_r}$$

其中整数  $d_i$  满足整除链条件:

$$d_1 \mid d_2 \mid \cdots \mid d_r \quad (d_1 > 1)$$

**例 2.2** (72 阶阿贝尔群的分类).  $72 = 2^3 \times 3^2$ . 通过组合初等因子并应用 CRT, 我们可以列出所有情况:

初等因子形式 ( $p$ -群分解)	不变因子形式 ( $d_1 \mid d_2 \dots$ )	CRT 逻辑
$C_8 \oplus C_9$	$\cong C_{72}$	$8 \times 9 = 72$
$C_4 \oplus C_2 \oplus C_9$	$\cong C_2 \oplus C_{36}$	$C_2 \oplus (C_4 \times C_9)$
$C_2 \oplus C_2 \oplus C_2 \oplus C_9$	$\cong C_2 \oplus C_2 \oplus C_{18}$	$C_2^2 \oplus (C_2 \times C_9)$
$C_8 \oplus C_3 \oplus C_3$	$\cong C_3 \oplus C_{24}$	$C_3 \oplus (C_8 \times C_3)$
$C_4 \oplus C_2 \oplus C_3 \oplus C_3$	$\cong C_6 \oplus C_{12}$	$(C_2 \times C_3) \oplus (C_4 \times C_3)$
$C_2^3 \oplus C_3^2$	$\cong C_2 \oplus C_6 \oplus C_6$	$C_2 \oplus (C_2 C_3) \oplus (C_2 C_3)$

## 3 结构定理的证明: 初级分解

### 补充详细证明

有限阿贝尔群结构定理的证明分为三步, 这里详细给出 \*\* 第一步 \*\* 的证明。

**定理 3.1** (初级分解定理). 设  $G$  是  $n$  阶有限阿贝尔群, 其素数分解为  $n = p_1^{e_1} \cdots p_k^{e_k}$ . 则  $G$  同构于其 Sylow  $p$ -子群的直和:

$$G \cong P_1 \oplus P_2 \oplus \cdots \oplus P_k$$

其中  $P_i = \{x \in G \mid p_i^{e_i} x = 0\}$  是  $G$  中所有阶为  $p_i$  的方幂的元素构成的子群。

证明. 我们将通过构造法证明  $G$  是  $P_i$  的直和。

### 1. 构造算子 (利用裴蜀定理)

令  $m_i = n/p_i^{e_i}$ 。由于  $p_1, \dots, p_k$  互不相同, 显然  $\gcd(m_1, m_2, \dots, m_k) = 1$ 。根据裴蜀定理 (Bézout's Identity), 存在整数  $s_1, s_2, \dots, s_k$  使得:

$$\sum_{i=1}^k s_i m_i = 1$$

### 2. 元素的分解

对于  $G$  中任意元素  $x$ , 我们可以利用上述等式将其分解:

$$x = 1 \cdot x = \left( \sum_{i=1}^k s_i m_i \right) x = \sum_{i=1}^k (s_i m_i x)$$

令  $x_i = s_i m_i x$ 。我们通过验证  $x_i$  的阶来证明  $x_i \in P_i$ 。计算  $p_i^{e_i} x_i$ :

$$p_i^{e_i} x_i = p_i^{e_i} (s_i m_i x) = s_i (p_i^{e_i} m_i) x = s_i n x$$

由于  $|G| = n$ , 根据拉格朗日定理,  $n x = 0$ 。因此  $p_i^{e_i} x_i = 0$ 。根据  $P_i$  的定义, 这意味着  $x_i \in P_i$ 。至此, 我们证明了  $G = P_1 + P_2 + \dots + P_k$ 。

### 3. 分解的唯一性 (直和的条件)

为了证明是直和, 我们需要证明交集为零。即证明  $P_i \cap (\sum_{j \neq i} P_j) = \{0\}$ 。假设  $y \in P_i \cap (\sum_{j \neq i} P_j)$ 。

- 一方面, 因为  $y \in P_i$ , 所以  $y$  的阶整除  $|P_i| = p_i^{e_i}$ 。
- 另一方面, 因为  $y \in \sum_{j \neq i} P_j$ , 所以  $y$  是其他  $P_j$  中元素之和。由于阿贝尔群中元素的阶等于各分量阶的最小公倍数,  $y$  的阶必须整除  $\prod_{j \neq i} |P_j| = m_i$ 。

因为  $\gcd(p_i^{e_i}, m_i) = 1$ , 所以  $y$  的阶必须为 1, 即  $y = 0$ 。

结论: 由于  $G$  是  $P_i$  的和, 且表示唯一 (交集为零), 故  $G \cong P_1 \oplus \dots \oplus P_k$ 。  $\square$

#### 直观理解: 证明思路总结

整个证明的核心在于利用  $n$  的因子互质性质, 通过  $\sum s_i m_i = 1$  将群中的“单位元”分解, 从而将任意元素  $x$  “投影”到各个  $p$ -分量上。



## 4 结构定理的证明：从初等因子到不变因子

### 证明第三步：重组算法

在完成了第一步（初级分解）和第二步（ $p$ -群的循环分解，此处略去其证明细节）后，我们已经知道任意有限阿贝尔群  $G$  可以分解为素数幂阶循环群的直和（即初等因子分解）。

本节的目标是证明：如何通过中国剩余定理 (CRT)，将这些“初等因子”重组为满足整除链条件的“不变因子”。

#### 4.1 算法目标

将形式为  $\bigoplus C_{p_i^{\alpha_{ij}}}$  的初等因子分解，转化为：

$$G \cong C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_r}$$

且满足  $d_1 \mid d_2 \mid \cdots \mid d_r$ 。

#### 4.2 重组算法 (Recombination Algorithm)

这是一个纯组合的过程。假设  $G$  的初等因子分解已完成，涉及的素数为  $p_1, p_2, \dots, p_k$ 。

**步骤 1：列表与排序** 将每个素数  $p_i$  对应的循环群阶数（即  $p_i$  的幂次）单列一行，并按从大到小的顺序排列。如果某一行元素较少，用 1（即  $C_1 = \{0\}$ ）在右侧补齐，使得每行长度一致。

素数	第 1 列 (最大)	第 2 列 (次大)	...	第 r 列 (最小)
$p_1$	$p_1^{\alpha_1}$	$p_1^{\alpha_2}$	...	$p_1^{\alpha_r}$
$p_2$	$p_2^{\beta_1}$	$p_2^{\beta_2}$	...	$p_2^{\beta_r}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$p_k$	$p_k^{\gamma_1}$	$p_k^{\gamma_2}$	...	$p_k^{\gamma_r}$

其中  $\alpha_1 \geq \alpha_2 \geq \dots, \beta_1 \geq \beta_2 \geq \dots$ 。

**步骤 2：纵向合并 (构造  $d_i$ )** 根据中国剩余定理，不同素数的幂次互质，因此它们的直积同构于其乘积的循环群：

$$C_{p_1^{\alpha_j}} \oplus C_{p_2^{\beta_j}} \oplus \cdots \oplus C_{p_k^{\gamma_j}} \cong C_{p_1^{\alpha_j} \cdot p_2^{\beta_j} \cdots p_k^{\gamma_j}}$$

我们将每一列的数相乘，定义为  $d_{r-j+1}$ （注意：为了符合  $d_1|d_2$  的习惯，通常将第一列最大的积作为最后一个因子  $d_r$ ）。

$$d_r = \prod p_i^{\text{max\_power}}, \quad d_{r-1} = \prod p_i^{\text{2nd\_max\_power}}, \quad \dots$$

### 4.3 整除性的验证

我们需要验证  $d_{r-1} \mid d_r$ 。

证明. 考察  $d_r$  和  $d_{r-1}$  的素因子分解：

$$d_r = p_1^{\alpha_1} p_2^{\beta_1} \cdots, \quad d_{r-1} = p_1^{\alpha_2} p_2^{\beta_2} \cdots$$

由于我们在步骤 1 中对每一行进行了降序排列，即：

$$\alpha_2 \leq \alpha_1, \quad \beta_2 \leq \beta_1, \quad \dots$$

这意味着对于每一个素因子  $p_i$ ，其在  $d_{r-1}$  中的幂次都小于等于在  $d_r$  中的幂次。因此，显然有  $d_{r-1} \mid d_r$ 。同理可证  $d_1 \mid d_2 \mid \cdots \mid d_r$ 。□

至此，我们完成了从初等因子到不变因子的转换证明。

#### 直观理解：总结：局部与整体的对偶性

有限阿贝尔群的两种分解形式揭示了群结构的两个侧面，它们通过 CRT 等价互推：

- **初等因子分解 (Elementary Divisors)**：体现了群的局部性质 (Local Structure)。它关注群在每一个素数  $p$  上的“微观结构”（即 Sylow  $p$ -子群的形态）。
- **不变因子分解 (Invariant Factors)**：体现了群的整体性质 (Global Structure)。其中最大的不变因子  $d_r$  实际上是群的指数 (Exponent)（即群中元素能达到的最大阶）。

## 5 商群构建：正规子群与商群 (笔记 P2-P4)

### 核 心 概 念：为何引入正规子群？

本节介绍群论中构建新群的另一种核心方法：\*\*商群 (Quotient Group)\*\*。

## 5.1 为什么要引入“正规子群”？

1. 核心问题：陪集乘法何时有效？我们知道子群  $H$  可以把群  $G$  划分成若干个陪集（如  $aH$ ）。我们想定义陪集间的运算：

$$(aH) \cdot (bH) := (ab)H$$

\*\* 问题 \*\*：这个定义是“良定”的（Well-defined）吗？即，换个代表元（ $a' \in aH$ ），结果是否改变？

### 2. 正规子群的定义

定义 5.1 (正规子群 Normal Subgroup). 子群  $N \subseteq G$  被称为正规子群（记作  $N \trianglelefteq G$ ），如果对于任意  $a \in G$ ，都有：

$$aN a^{-1} = N \quad (\text{等价于 } aN = Na)$$

### 3. 验证推导

$$(aH)(bH) = a(Hb)H = a(bH)H = ab(HH) = abH$$

只有当  $Hb = bH$ （正规性）时，中间的  $b$  才能“穿”过去， $H$  才能合并。

## 5.2 商群的定义与例子

定义 5.2 (商群 Quotient Group). 若  $N \trianglelefteq G$ ，则集合  $G/N = \{aN \mid a \in G\}$  构成一个群：

- 单位元： $e_{G/N} = N$ 。
- 乘法： $(aN)(bN) = abN$ 。
- 逆元： $(aN)^{-1} = a^{-1}N$ 。

术语：我们称  $G$  是  $G/N$  被  $N$  的扩张 (Extension)。

例 5.3 (经典例子).

- 整数模  $n$ :  $G = \mathbb{Z}, N = n\mathbb{Z}$ 。商群  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$ 。

- 射影线性群： $PGL_n(k) \cong GL_n(k)/k^\times$ 。这里的  $k^\times$  指标量矩阵中心  $Z$ 。

## 6 商群的严格证明与第一同构定理基础 (笔记 P6, P7)

### 商群的构成证明

## 6.1 运算良定性的详细证明

设  $N \trianglelefteq G$ 。我们要证明  $(ab)N$  不依赖于代表元的选择。

证明. 假设  $aN = a'N$  且  $bN = b'N$ 。这意味着  $a^{-1}a' \in N$  且  $b^{-1}b' \in N$ 。考察  $(ab)^{-1}(a'b')$ :

$$\begin{aligned}(ab)^{-1}(a'b') &= b^{-1}a^{-1}a'b' \\ &= b^{-1} \underbrace{(a^{-1}a')}_{\in N} b' \\ &= \underbrace{b^{-1}(a^{-1}a')b}_{\in N \text{ (因正规性)}} \cdot \underbrace{(b^{-1}b')}_{\in N} \in N\end{aligned}$$

因此  $(ab)N = (a'b')N$ ，运算良定。 □

## 6.2 核与正规子群的关系

**命题 6.1.** 正规子群本质上就是群同态的核。

设群  $G$  作用在集合  $X$  上。定义  $N$  为该作用的 \*\* 核 (Kernel of Action)\*\*:

$$N \triangleq C_G(X) = \{g \in G \mid g \cdot x = x, \forall x \in X\}$$

则  $N$  是  $G$  的正规子群。商群  $G/N$  同构于  $G$  在  $S(X)$  中的像 (单射嵌入)。

## 6.3 经典同构关系

利用同态基本定理，我们有：

- $S_n/A_n \cong C_2$  (奇偶置换)。
- $GL_n(k)/SL_n(k) \cong k^\times$  (行列式映射)。
- $O(n)/SO(n) \cong C_2$ 。

## 7 第一同构定理：泛性质与同构 (笔记 P8, P9)

### 定理陈述与证明

## 7.1 诱导同态的存在性 (泛性质)

**定理 7.1.** 设  $\Phi: G \rightarrow G'$  是群同态,  $N \trianglelefteq G$ 。若  $N \subseteq \ker(\Phi)$ , 则存在 **\*\*唯一\*\*** 的同态  $\bar{\Phi}: G/N \rightarrow G'$  使得  $\bar{\Phi} \circ \pi = \Phi$ 。

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & G' \\ \pi \downarrow & \nearrow \bar{\Phi} & \\ G/N & & \end{array}$$

证明. **1. 定义:**  $\bar{\Phi}(aN) = \Phi(a)$ 。**2. 良定性:** 若  $aN = bN$ , 则  $b^{-1}a \in N \subseteq \ker(\Phi)$ 。故  $\Phi(b^{-1}a) = e'$ , 即  $\Phi(a) = \Phi(b)$ 。**3. 唯一性:** 由  $\pi$  的满射性易证。□

## 7.2 第一同构定理

**定理 7.2** (First Isomorphism Theorem). 若取  $N = \ker(\Phi)$ , 则诱导同态  $\bar{\Phi}$  是一个同构:

$$G/\ker(\Phi) \cong \text{Im}(\Phi)$$

直观理解: 直观理解

任何同态都可以分解为: 商映射 (压缩)  $\rightarrow$  同构映射 (一一对应)  $\rightarrow$  包含映射。

## 7.3 第一同构定理的详细证明

**定理 7.3** (First Isomorphism Theorem). 设  $\Phi: G \rightarrow G'$  是一个群同态, 其核为  $K = \ker(\Phi)$ 。则映射

$$\bar{\Phi}: G/K \rightarrow \text{Im}(\Phi)$$

定义为  $\bar{\Phi}(gK) = \Phi(g)$ , 是一个群同构。即:

$$G/\ker(\Phi) \cong \text{Im}(\Phi)$$

证明. 我们需要验证  $\bar{\Phi}$  满足同构的三个条件: 良定且保持运算 (同态)、满射、单射。

**1. 良定性与同态性质 (Well-defined Homomorphism)** 由上一小节 (诱导同态的存在性) 可知, 由于  $K = \ker(\Phi)$ , 映射  $\bar{\Phi}$  是良定的群同态。

**2. 满射性 (Surjectivity)** 我们要证明  $\text{Im}(\Phi)$  中的每一个元素都能被  $\bar{\Phi}$  映射到。

- 取任意  $y \in \text{Im}(\Phi)$ 。

- 根据像的定义，存在  $g \in G$  使得  $\Phi(g) = y$ 。
- 考虑  $G/K$  中的陪集  $gK$ ，根据定义有  $\bar{\Phi}(gK) = \Phi(g) = y$ 。
- 因此， $\bar{\Phi}$  是满射。

**3. 单射性 (Injectivity)** 我们要证明  $\bar{\Phi}$  的核  $\ker(\bar{\Phi})$  只有  $G/K$  的单位元（即  $K$  本身）。  
 设  $gK \in G/K$  是  $\bar{\Phi}$  核中的元素：

$$\begin{aligned}
 gK \in \ker(\bar{\Phi}) &\iff \bar{\Phi}(gK) = e' \quad (e' \text{ 是 } G' \text{ 的单位元}) \\
 &\iff \Phi(g) = e' \quad (\text{映射定义}) \\
 &\iff g \in \ker(\Phi) \quad (\text{核的定义}) \\
 &\iff g \in K \\
 &\iff gK = K \quad (\text{子群陪集的性质})
 \end{aligned}$$

由于  $\ker(\bar{\Phi}) = \{K\}$ （即商群的单位元），故  $\bar{\Phi}$  是单射。

结论：由于  $\bar{\Phi}$  既是单射又是满射的同态，因此它是同构。 □

#### 直观理解：直观理解：纤维 (Fibers) 的塌缩

群同态  $\Phi$  将  $G$  分割成了一束束的“纤维” (Fibers)。

- 每一个纤维就是  $K$  的一个陪集  $gK$ 。
- 同一个纤维  $gK$  里的所有元素，通过  $\Phi$  都被“压缩”到了  $G'$  中的同一点  $\Phi(g)$  上。
- \*\* 第一同构定理 \*\* 说的是：如果我们把每个纤维看作一个点（即商群  $G/K$ ），那么这个新的结构与像集  $\text{Im}(\Phi)$  是一模一样的（同构）。

## 8 约化映射 (Reduction Map) (笔记 P12)

### 从大商群到小商群

本节展示如何把一个“较大”的商群 ( $N_0$  小) 映射到一个“较小”的商群 ( $H$  大)。

## 8.1 整数模 $n$ 到模 $d$ 的映射

- 条件:  $d \mid n$  (即  $n\mathbb{Z} \subseteq d\mathbb{Z}$ )。
- 映射:  $\pi_{n,d}: \mathbb{Z}_n \rightarrow \mathbb{Z}_d$ , 定义为  $a \pmod n \mapsto a \pmod d$ 。
- 存在性: 因为  $n\mathbb{Z} \subseteq \ker(\text{mod } d)$ , 根据诱导同态定理, 该映射良定。

## 8.2 一般化推广

设  $N_0 \trianglelefteq G, H \trianglelefteq G$ , 且  $**N_0 \subseteq H^{**}$ 。存在自然满同态:

$$\bar{\pi}: G/N_0 \rightarrow G/H, \quad aN_0 \mapsto aH$$

直观理解:  $N_0$  的陪集是“小盒子”,  $H$  的陪集是“大盒子”。因为  $N_0 \subseteq H$ , 每个小盒子都完全包含在某个大盒子里, 所以可以直接把小盒子“扔进”大盒子。

## 9 换位子、导群与特征子群 (笔记 P13, P14)

### 群的“非阿贝尔程度”与强不变性

### 9.1 换位子与导群

定义 9.1 (换位子 Commutator). 元素  $a, b$  的换位子为  $(a, b) = aba^{-1}b^{-1}$ 。

定义 9.2 (导群 Derived Subgroup). 由  $G$  中  $**$  所有  $**$  换位子生成的子群:

$$G^{(1)} = G' = \langle \{aba^{-1}b^{-1} \mid a, b \in G\} \rangle$$

- $S'_n = A_n$  ( $n \geq 3$ )。
- $\text{GL}_n(k)' = \text{SL}_n(k)$  ( $n \geq 2$ )。

### 9.2 经典导群例子的详细证明

例 9.3 (对称群的导群). 对于  $n \geq 3$ , 有  $(S_n)^{(1)} = A_n$ 。

证明. 我们需要证明双向包含:  $S'_n \subseteq A_n$  和  $A_n \subseteq S'_n$ 。

**1. 证明  $S'_n \subseteq A_n$**  利用符号同态  $\text{sgn} : S_n \rightarrow \{1, -1\}$ 。我们知道  $A_n = \ker(\text{sgn})$ 。对于任意换位子  $x = aba^{-1}b^{-1}$ , 应用同态性质:

$$\text{sgn}(x) = \text{sgn}(a)\text{sgn}(b)\text{sgn}(a)^{-1}\text{sgn}(b)^{-1} = 1$$

因此, 所有换位子都是偶置换。由换位子生成的群  $S'_n$  必包含于  $A_n$ 。

**2. 证明  $A_n \subseteq S'_n$**  已知对于  $n \geq 3$ , 交错群  $A_n$  是由所有的 \*\*3-轮换 (3-cycles)\*\* 生成的。我们只需证明任意 3-轮换都是一个换位子即可。考虑 3-轮换  $(ijk)$ 。取  $S_n$  中的对换  $\sigma = (ij)$  和  $\tau = (ik)$  (注意  $n \geq 3$  保证了下标互异的可行性)。计算它们的换位子:

$$[\sigma, \tau] = (ij)(ik)(ij)^{-1}(ik)^{-1} = (ij)(ik)(ij)(ik)$$

按映射顺序 (从右向左作用):

- $i \xrightarrow{(ik)} k \xrightarrow{(ij)} k$
- $k \xrightarrow{(ik)} i \xrightarrow{(ij)} j$
- $j \xrightarrow{(ik)} j \xrightarrow{(ij)} i$

即  $[\sigma, \tau] = (ikj) = (jik)^{-1}$ 。或者使用笔记中的构造:  $(123) = [(12), (13)^{-1}]$  (取决于乘法习惯, 本质一样)。既然任意 3-轮换都能写成换位子, 故  $A_n \subseteq S'_n$ 。

**结论:**  $S'_n = A_n$ 。 □

**例 9.4** (一般线性群的导群). 对于  $n \geq 2$  (且基域  $k$  不是  $\mathbb{F}_2$  的极端情况), 有  $(\text{GL}_n(k))^{(1)} = \text{SL}_n(k)$ 。

证明. 同样证明双向包含。

**1. 证明  $\text{GL}'_n \subseteq \text{SL}_n$**  利用行列式同态  $\det : \text{GL}_n(k) \rightarrow k^\times$ 。我们知道  $\text{SL}_n(k) = \ker(\det)$ 。对于任意矩阵换位子  $[A, B] = ABA^{-1}B^{-1}$ :

$$\det([A, B]) = \det(A)\det(B)\det(A)^{-1}\det(B)^{-1} = 1$$

因此所有换位子都在  $\text{SL}_n(k)$  中, 故  $\text{GL}'_n \subseteq \text{SL}_n$ 。

**2. 证明  $\text{SL}_n \subseteq \text{GL}'_n$**  线性代数告诉我们,  $\text{SL}_n(k)$  由 \*\*初等矩阵\*\* (Transvections, 形如  $E_{ij}(\lambda) = I + \lambda e_{ij}, i \neq j$ ) 生成。我们需要证明任何初等矩阵都是  $\text{GL}_n(k)$  中的换位子。

取对角矩阵  $D = \text{diag}(u, 1, \dots, 1) \in \text{GL}_n(k)$  和初等矩阵  $E = E_{12}(1)$ 。计算共轭  $DED^{-1}$ :

$$\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = E_{12}(u)$$



考察换位子  $[D, E]$ :

$$[D, E] = (DED^{-1})E^{-1} = E_{12}(u)E_{12}(-1) = E_{12}(u-1)$$

只要域  $k$  中有足够多的元素 ( $|k| > 2$ ), 我们总能找到  $u$  使得  $u-1 = \lambda$  为任意值。因此, 初等矩阵均可表示为换位子 (对于  $n \geq 3$ , 甚至可以用两个初等矩阵的换位子直接生成)。

结论:  $GL'_n = SL_n$ 。 □

### 9.3 特征子群 (Characteristic Subgroup)

**定义 9.5.** 若子群  $H$  在  $G$  的 \*\*所有\*\* 自同构 (不仅是内自同构) 下不变, 即  $\forall \sigma \in \text{Aut}(G), \sigma(H) = H$ , 则称  $H$  为  $G$  的特征子群, 记作  $H \text{ char } G$ 。

显然: 特征子群  $\implies$  正规子群。

### 9.4 重要性质与证明

**命题 9.6** (传递性).

1.  $H_0 \text{ char } H_1, H_1 \trianglelefteq G \implies H_0 \trianglelefteq G$ 。
2.  $H_0 \text{ char } H_1, H_1 \text{ char } G \implies H_0 \text{ char } G$ 。

### 9.5 特征子群性质的详细证明

**命题 9.7** (特征子群的传递规律).

1. 混合传递性:  $H_0 \text{ char } H_1, H_1 \trianglelefteq G \implies H_0 \trianglelefteq G$ 。
2. 完全传递性:  $H_0 \text{ char } H_1, H_1 \text{ char } G \implies H_0 \text{ char } G$ 。

**证明性质 1:**  $H_0 \text{ char } H_1, H_1 \trianglelefteq G \implies H_0 \trianglelefteq G$ . 我们要证明对于任意  $g \in G$ , 都有  $gH_0g^{-1} = H_0$ 。

**1. 构造共轭映射** 任取  $g \in G$ . 定义  $G$  上的共轭映射 (内自同构)  $\phi_g : G \rightarrow G$ , 其中  $\phi_g(x) = gxg^{-1}$ 。

2. 限制在  $H_1$  上由于  $H_1 \trianglelefteq G$  (正规子群),  $H_1$  在  $G$  的共轭作用下是封闭的。即对于任意  $h \in H_1$ ,  $\phi_g(h) = ghg^{-1} \in H_1$ 。因此, 我们可以将  $\phi_g$  限制在  $H_1$  上, 得到映射:

$$\phi_g|_{H_1} : H_1 \rightarrow H_1$$

这是一个从  $H_1$  到  $H_1$  的双射同态, 即  $\phi_g|_{H_1} \in \text{Aut}(H_1)$ 。

3. 利用特征子群定义已知  $H_0 \text{ char } H_1$ 。这意味着  $H_0$  在  $H_1$  的任意自同构下都不变。因为  $\phi_g|_{H_1}$  是  $H_1$  的一个自同构, 所以:

$$\phi_g|_{H_1}(H_0) = H_0$$

即  $gH_0g^{-1} = H_0$ 。

结论:  $H_0 \trianglelefteq G$ 。 □

证明性质 2:  $H_0 \text{ char } H_1, H_1 \text{ char } G \implies H_0 \text{ char } G$ . 我们要证明对于  $G$  的任意自同构  $\sigma \in \text{Aut}(G)$ , 都有  $\sigma(H_0) = H_0$ 。

1. 第一层限制 ( $H_1$  的不变性) 任取  $\sigma \in \text{Aut}(G)$ 。因为  $H_1 \text{ char } G$ , 根据定义  $\sigma(H_1) = H_1$ 。这意味着  $\sigma$  可以限制在  $H_1$  上, 得到限制映射:

$$\sigma|_{H_1} : H_1 \rightarrow H_1$$

这也是一个同构映射, 即  $\sigma|_{H_1} \in \text{Aut}(H_1)$ 。

2. 第二层限制 ( $H_0$  的不变性) 因为  $H_0 \text{ char } H_1$ , 这意味着  $H_0$  在  $H_1$  的任意自同构下不变。应用到上述的限制映射  $\sigma|_{H_1}$ , 我们有:

$$\sigma|_{H_1}(H_0) = H_0$$

结论: 这等价于  $\sigma(H_0) = H_0$ 。由于  $\sigma$  是任意选取的, 故  $H_0 \text{ char } G$ 。 □

**直观理解: 辨析: 为什么正规子群不具备传递性?**

如果只知道  $H_0 \trianglelefteq H_1 \trianglelefteq G$ :

- $G$  的共轭作用  $\phi_g$  虽然把  $H_1$  映回  $H_1$ , 但这对于  $H_1$  来说可能是一个 \*\* 外自同构 \*\* (Outer Automorphism)。
- $H_0 \trianglelefteq H_1$  只能保证  $H_0$  在  $H_1$  的 \*\* 内自同构 \*\* 下不变, 无法保证它在  $\phi_g|_{H_1}$  这种潜在的外自同构下不变。
- \*\* 特征子群 \*\* 的定义更强 (对所有自同构不变), 因此弥补了这个漏洞。

### 注意 (NOTE): 反例

正规子群不具有传递性:  $H_0 \trianglelefteq H_1 \trianglelefteq G \not\Rightarrow H_0 \trianglelefteq G$ 。例如  $V_4 \trianglelefteq S_4$ , 但  $V_4$  的子群  $\{e, (12)(34)\}$  在  $S_4$  中不正规。

## 10 群的直积与泛性质 (笔记 P16, P20)

### 组装与拆解群的终极工具

### 10.1 外直积 (External Direct Product) —— 组装

给定群  $G_1, \dots, G_r$ , 其直积  $(g_1, \dots, g_r)$  构成新群。原群  $G_i$  可视作正规子群嵌入其中。

### 10.2 内直积 (Internal Direct Product) —— 拆解判据

定理 10.1 (内直积判别准则). 群  $G$  同构于子群  $N_1 \times \dots \times N_r$  的充要条件是:

1. 正规性:  $\forall i, N_i \trianglelefteq G$ 。
2. 生成性:  $G = N_1 \cdot N_2 \cdots N_r$ 。
3. 独立性:  $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_r) = \{e\}$ 。

#### 直观理解: 为什么子群元素必须能交换?

对于  $r = 2$ , 若  $G \cong N_1 \times N_2$ , 则  $n_1 \in N_1, n_2 \in N_2$  必须交换。证明: 考察换位子  $x = n_1 n_2 n_1^{-1} n_2^{-1}$ 。

- 因  $N_2$  正规,  $x = n_1(n_2 n_1^{-1} n_2^{-1}) \in N_1$  (?? 修正: 此处应结合正规性分析)。
- 更准确地:  $x = (n_1 n_2 n_1^{-1}) n_2^{-1} \in N_2$ ; 且  $x = n_1(n_2 n_1^{-1} n_2^{-1}) \in N_1$ 。
- 故  $x \in N_1 \cap N_2$ 。由独立性,  $N_1 \cap N_2 = \{e\}$ , 故  $x = e$ , 即  $n_1 n_2 = n_2 n_1$ 。

### 10.3 泛性质 (Universal Property)

群的直积  $P = G_1 \times \cdots \times G_r$  具有以下泛性质：对于任意群  $H$  和一族同态  $\phi_i : H \rightarrow G_i$ ，存在 \*\* 唯一 \*\* 的同态  $\Phi : H \rightarrow P$  使得  $\pi_i \circ \Phi = \phi_i$ 。

$$\Phi(h) = (\phi_1(h), \dots, \phi_r(h))$$

只要确定了去往各个分量的路径，去往直积群的路径也就唯一确定了。

## 本章导读

本文档整理了关于群论结构的进阶内容，涵盖以下核心主题：

- **矩阵群的分解**：从几何变换角度理解上三角矩阵群的结构。
- **半直积 (Semi-direct Product)**：通过  $D_n$  和  $S_4$  等例子理解群的“拆解”与“组装”。
- **同构定理**：详细推导对应定理、第三同构定理及第二同构定理（钻石定理）。
- **有限群分类**：6 阶与 8 阶群的完全分类，特别是  $D_4$  与  $Q_8$  的辨析。

## 11 矩阵群与短正合列 (Matrix Groups)

在一般线性群  $GL_n(k)$  中，我们可以定义以下重要的子群结构。

定义 11.1 (矩阵子群). 1. 上三角矩阵群 (*Upper Triangular Group*)  $\mathbb{T}_n(k)$ :

$$\mathbb{T}_n(k) = \left\{ \begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix} \in GL_n(k) \right\}$$

2. 对角矩阵群 (*Diagonal Group*)  $\mathbb{D}_n(k)$ :

$$\mathbb{D}_n(k) = \left\{ \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\} \cong (k^\times)^n$$

3. 么幂群 (*Unipotent Group*)  $\mathbb{U}_n(k)$ :

$$\mathbb{U}_n(k) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$$

这些群之间满足包含关系： $\mathbb{U}_n(k) \leq \mathbb{T}_n(k) \leq GL_n(k)$ 。

### 11.1 补充：短正合列详解与实例分析

为了深入理解矩阵群的结构，我们需要从代数定义的角度严格剖析短正合列。

### 11.1.1 短正合列的形式化定义

**定义 11.2** (正合序列). 一个群同态序列  $\cdots \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow \cdots$  称为在  $B$  处正合 (*Exact*), 如果前一个映射的像等于后一个映射的核, 即:

$$\text{Im}(f) = \ker(g)$$

**定义 11.3** (短正合列). 如下形式的序列称为短正合列 (*Short Exact Sequence*):

$$1 \rightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \rightarrow 1$$

它蕴含了三个关键信息:

1.  $i$  是单射 ( $\ker(i) = \{1\}$ ): 即  $N$  同构于  $G$  的一个子群。
2.  $\pi$  是满射 ( $\text{Im}(\pi) = Q$ ): 即  $Q$  是商群的同构像。
3. 核心正合性 ( $\text{Im}(i) = \ker(\pi)$ ): 即  $N$  在  $G$  中的像恰好是  $\pi$  的核。这也意味着  $N$  必须是  $G$  的正规子群。

综上, 短正合列等价于群同构定理:  $G/N \cong Q$ 。

### 11.1.2 矩阵群序列的具体分析

让我们具体分析笔记中的序列:

$$1 \rightarrow \mathbb{U}_n(k) \xrightarrow{i} \mathbb{T}_n(k) \xrightarrow{\pi} \mathbb{D}_n(k) \rightarrow 1$$

**1. 映射  $i$  (包含映射 Inclusion):**

$$i: \mathbb{U}_n(k) \rightarrow \mathbb{T}_n(k), \quad A \mapsto A$$

显然, 幺幂矩阵也是上三角矩阵。 $i$  是单射是显然的。

**2. 映射  $\pi$  (投影映射 Projection):** 定义映射  $\pi$  为“取对角元”:

$$\pi \left( \begin{pmatrix} a_{11} & * & * \\ 0 & \ddots & * \\ 0 & 0 & a_{nn} \end{pmatrix} \right) = \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_{nn} \end{pmatrix}$$

- **同态性验证:** 上三角矩阵乘积的对角元只取决于对角元的乘积 ( $(AB)_{kk} = A_{kk}B_{kk}$ )。因此  $\pi(AB) = \pi(A)\pi(B)$ 。

- **满射性验证:** 任取  $D \in \mathbb{D}_n(k)$ , 显然  $D \in \mathbb{T}_n(k)$  (对角阵也是上三角阵), 且  $\pi(D) = D$ 。

**3. 核心正合性验证 ( $\ker(\pi) = \mathbb{U}_n$ ):** 我们要寻找  $\pi$  的核, 即哪些矩阵映射后变成了单位阵  $I$ 。

$$\pi(A) = I \iff \begin{pmatrix} a_{11} & 0 \\ 0 & \ddots \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

这要求  $A$  的对角元  $a_{kk}$  全部为 1。

$$A = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

这正是么幂群  $\mathbb{U}_n(k)$  的定义!

$$\therefore \ker(\pi) = \mathbb{U}_n(k)$$

#### 直观理解: 直观总结

这个短正合列告诉我们:

- **整体 ( $G$ ):** 上三角矩阵群  $\mathbb{T}_n$ 。
- **商 ( $Q$ ):** 如果我们忽略掉矩阵右上角的元素 (即把它们看作 0, 或者说模掉), 剩下的骨架就是对角矩阵群  $\mathbb{D}_n$ 。
- **核 ( $N$ ):** 那些被“忽略”掉的差异, 正是主对角线为 1 的矩阵 ( $\mathbb{U}_n$ ), 它们代表了纯粹的“形变”而不包含“伸缩”。

## 12 半直积 (Semi-direct Product)

### 群的“拆解”与“组装”新工具

半直积是直积的推广。在直积中, 两个子群都是正规的; 而在半直积中, 我们只需要其中一个正规子群。这使得我们能够将更多的群“拆解”为简单的部分。

## 12.1 外半直积 (构造篇)

**场景：**给定两个独立的群  $N$  和  $H$ ，我们想把它们拼成一个大群。为了让结构不那么平凡（不是直积），我们引入一个同态  $\varphi: H \rightarrow \text{Aut}(N)$ ，即  $H$  通过  $\varphi$  作用在  $N$  上。

**定义 12.1** (外半直积的定义). 设  $N, H$  是群,  $\varphi: H \rightarrow \text{Aut}(N)$  是群同态。定义集合  $G = N \rtimes H = \{(n, h) \mid n \in N, h \in H\}$ 。定义乘法运算如下（注意扭曲项）：

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \varphi(h_1)(n_2), h_1 h_2)$$

这样构成的群称为  $N$  与  $H$  关于  $\varphi$  的外半直积，记为  $N \rtimes_{\varphi} H$ 。

**定理 12.2** (群公理的验证). 上述定义的  $(G, \cdot)$  确实构成一个群。

**证明.** 我们需要验证结合律、单位元和逆元。

1. **结合律 (Associativity):** 令  $x = (n_1, h_1), y = (n_2, h_2), z = (n_3, h_3)$ 。记  $n^h = \varphi(h)(n)$ 。

首先计算  $(xy)z$ ：

$$(xy)z = (n_1 n_2^{h_1}, h_1 h_2) \cdot (n_3, h_3) = (n_1 n_2^{h_1} n_3^{h_1 h_2}, h_1 h_2 h_3)$$

然后计算  $x(yz)$ ：

$$x(yz) = (n_1, h_1) \cdot (n_2 n_3^{h_2}, h_2 h_3) = (n_1 (n_2 n_3^{h_2})^{h_1}, h_1 h_2 h_3)$$

关键在于展开  $x(yz)$  中的  $N$  部分。由于  $\varphi(h_1)$  是自同构（保持乘法），且  $\varphi$  是同态（保持群作用顺序）：

$$(n_2 n_3^{h_2})^{h_1} = n_2^{h_1} (n_3^{h_2})^{h_1}$$

根据左作用同态性质  $\varphi(h_1) \circ \varphi(h_2) = \varphi(h_1 h_2)$ ，我们有：

$$(n_3^{h_2})^{h_1} = n_3^{h_1 h_2}$$

因此：

$$x(yz) = (n_1 n_2^{h_1} n_3^{h_1 h_2}, h_1 h_2 h_3)$$

对比可知  $(xy)z = x(yz)$ ，结合律成立。

2. **单位元 (Identity):**  $e_G = (e_N, e_H)$ 。容易验证  $(n, h)(e_N, e_H) = (n \cdot e_N^h, h) = (n, h)$ 。

3. **逆元 (Inverse):** 元素  $(n, h)$  的逆元为  $(\varphi(h^{-1})(n^{-1}), h^{-1})$ 。

□



## 12.2 内半直积 (识别篇)

场景：我们已经有一个大群  $G$ ，想看看它是不是由两个子群“拼”出来的。

定义 12.3 (内半直积条件). 设  $G$  是群,  $N \trianglelefteq G$  (正规子群),  $H \leq G$  (子群)。若满足：

1.  $G = NH$  (即  $\forall g \in G, g = nh$ );
2.  $N \cap H = \{e\}$  (交集平凡);

则称  $G$  是  $N$  和  $H$  的内半直积, 记为  $G \cong N \rtimes H$ 。

定理 12.4 (内外等价性). 若  $G$  满足内半直积条件, 则  $G \cong N \rtimes_{\varphi} H$ , 其中  $\varphi : H \rightarrow \text{Aut}(N)$  是共轭作用  $\varphi(h)(n) = hnh^{-1}$ 。

推导. 在群  $G$  中, 考虑两个元素  $n_1h_1$  和  $n_2h_2$  的乘积。我们需要将  $h_1$  移到  $n_2$  的右边。利用插值法 ( $h_1^{-1}h_1 = e$ ):

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1}h_1)h_2 = n_1(\underbrace{h_1n_2h_1^{-1}}_{\in N, \text{正规性}})(h_1h_2)$$

这正是外半直积定义的乘法规则。 □

### 注意 (NOTE): 半直积的核心哲学

外半直积的本质作用是：它将“两个群之间的相互作用 (Action)”固化为了“一个新的群结构”。

- **内半直积**：是发现已有的群里包含这种结构（类似于“事后诸葛亮”，用于拆解）。
- **外半直积**：是主动利用这种结构去创造新群（通过设计不同的  $\varphi$ ，类似于“乐高积木”）。

## 12.3 实例详解： $S_4$ 的分解

### 将对称群 $S_4$ 拆解为半直积

命题 12.5. 对称群  $S_4$  可以分解为半直积：  $S_4 \cong V_4 \rtimes S_3$ 。

我们需要找到一个正规子群  $N \cong V_4$  和一个子群  $H \cong S_3$ ，并验证内半直积的条件。

证明. **第一步：构造正规子群  $V_4$**  取  $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ 。

- 这是一个群（克莱因四元群）。
- **正规性验证：**在  $S_n$  中，共轭不改变循环型（Cycle Type）。 $V_4$  包含了  $S_4$  中所有型为  $(xx)(xx)$  的元素以及单位元。因此，任何  $\sigma \in S_4$  作用在  $V_4$  上，结果仍在  $V_4$  中。故  $V_4 \trianglelefteq S_4$ 。

**第二步：构造补子群  $S_3$**  取  $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$ （即固定元素 4 的所有置换）。

- 显然  $H$  同构于  $S_3$ （对  $\{1, 2, 3\}$  的全排列）。

**第三步：验证交集为  $\{e\}$**

- $H$  中的非单位元必须固定 4。
- $V_4$  中的非单位元都是双对换，例如  $(12)(34)$ ，它们都会把 4 变到 3、2 或 1，即  $\sigma(4) \neq 4$ 。
- 因此  $V_4 \cap H = \{e\}$ 。

**第四步：验证生成全群**

- 根据计数公式： $|V_4 H| = \frac{|V_4||H|}{|V_4 \cap H|} = \frac{4 \times 6}{1} = 24$ 。
- 而  $|S_4| = 24$ 。
- 因为  $V_4 H$  是  $S_4$  的子集且元素个数相等，故  $S_4 = V_4 H$ 。

**结论：**  $S_4$  满足所有内半直积条件，故  $S_4 \cong V_4 \rtimes S_3$ 。 □

## 13 同构定理的详细证明 (Isomorphism Theorems)

同构定理是群论的基石，它们建立了子群、商群与同态之间的桥梁。所有的证明核心都依赖于 \*\* 第一同构定理 \*\*：

$$G/\ker \varphi \cong \text{Im } \varphi$$

### 13.1 第三同构定理 (The Third Isomorphism Theorem)

别名：消去律定理 (Cancellation Law)

定理 13.1. 设  $N \trianglelefteq G, H \trianglelefteq G$  且  $N \subseteq H$ 。则  $H/N \trianglelefteq G/N$ ，且：

$$(G/N)/(H/N) \cong G/H$$

证明. 我们要利用第一同构定理，构造一个从大商群  $G/N$  到  $G/H$  的满同态。

第一步：构造映射定义  $\psi : G/N \rightarrow G/H$ ，规则为：

$$\psi(gN) = gH$$

第二步：验证良定义 (Well-defined) 设  $g_1N = g_2N$ ，即  $g_2^{-1}g_1 \in N$ 。由于  $N \subseteq H$ ，所以  $g_2^{-1}g_1 \in H$ ，这等价于  $g_1H = g_2H$ 。因此  $\psi(g_1N) = \psi(g_2N)$ ，映射与代表元选取无关。

第三步：验证同态与满射

- 同态：  $\psi(g_1N \cdot g_2N) = \psi(g_1g_2N) = g_1g_2H = (g_1H)(g_2H) = \psi(g_1N)\psi(g_2N)$ 。
- 满射： 对于任意  $y \in G/H$ ，可设  $y = gH$ 。显然  $\psi(gN) = gH$ 。

第四步：计算核 (Kernel)

$$\ker \psi = \{gN \in G/N \mid \psi(gN) = e_{G/H}\}$$

这里商群  $G/H$  的单位元是  $H$ 。

$$\psi(gN) = H \iff gH = H \iff g \in H$$

因此， $\ker \psi = \{gN \mid g \in H\} = H/N$ 。

结论：由第一同构定理  $Dom/\ker \cong Im$ ，得：

$$(G/N)/(H/N) \cong G/H$$

□

### 13.2 第二同构定理 (The Second Isomorphism Theorem)

别名：钻石定理 (Diamond Theorem)

**定理 13.2.** 设  $H \leq G$  (子群),  $N \trianglelefteq G$  (正规子群)。则:

1.  $HN$  是  $G$  的子群, 且  $N \trianglelefteq HN$ 。
2.  $H \cap N$  是  $H$  的正规子群。
3. 如下同构成立:

$$HN/N \cong H/(H \cap N)$$

**证明. 前置验证:** 首先,  $HN$  是子群 (已在半直积部分讨论过)。因为  $N \trianglelefteq G$ , 所以  $N \trianglelefteq HN$  显然成立。

**核心证明思路:** 我们要建立  $H$  和  $HN/N$  之间的联系。构造一个从  $H$  出发的同态。

**第一步: 构造映射** 定义  $\phi: H \rightarrow HN/N$ , 规则为:

$$\phi(h) = hN$$

即把  $h$  映射到它在  $HN$  中的陪集。

**第二步: 同态与满射**

- **同态:**  $\phi(h_1 h_2) = (h_1 h_2)N = h_1 N \cdot h_2 N = \phi(h_1) \phi(h_2)$ 。
- **满射:** 这是证明的关键。任取  $HN/N$  中的元素, 形式为  $(hn)N$ 。利用正规子群的吸收性质:  $(hn)N = h(nN) = hN$ 。这说明虽然代表元看起来是  $hn$ , 但其实  $h$  就能代表这个陪集。由于  $h \in H$ , 所以  $\phi(h) = hN$ , 即  $\phi$  是满射。

**第三步: 计算核 (Kernel)**

$$\ker \phi = \{h \in H \mid \phi(h) = N\}$$

$$hN = N \iff h \in N$$

因为定义域限制了  $h \in H$ , 所以:

$$\ker \phi = H \cap N$$

这也顺便证明了  $H \cap N \trianglelefteq H$  (因为核总是正规子群)。

**结论:** 由第一同构定理:

$$H/(H \cap N) \cong HN/N$$

□

## 14 有限群的分类 (Classification)

### 14.1 六阶群的分类

通过拉格朗日定理和柯西定理分析：

- 若存在 6 阶元  $\implies C_6$ 。
- 若不存在 6 阶元，必有 3 阶正规子群  $N$  和 2 阶子群  $H$ 。
- 构成的半直积  $C_3 \rtimes C_2$  非阿贝尔  $\implies S_3$ 。

结论：6 阶群只有  $C_6$  和  $S_3$  两种。

### 14.2 八阶群的分类

8 阶群共有 5 种：

1. 阿贝尔群 (3 种):  $C_8$ ,  $C_4 \times C_2$ ,  $C_2 \times C_2 \times C_2$ 。
2. 非阿贝尔群 (2 种):
  - 二面体群  $D_4$ : 正方形的对称群。
  - 四元数群  $Q_8$ :  $\{\pm 1, \pm i, \pm j, \pm k\}$ 。

**注意 (NOTE):** 如何区分  $D_4$  和  $Q_8$ ?

虽然它们都是 8 阶非阿贝尔群，且都有一个 4 阶正规子群，但可以通过统计元素阶数来区分：

阶数	$D_4$ 的元素个数	$Q_8$ 的元素个数
1 阶	1 ( $e$ )	1 (1)
2 阶	5 (中心 1 个 + 反射 4 个)	1 ( $-1$ )
4 阶	2	6 ( $\pm i, \pm j, \pm k$ )

$Q_8$  还有一个特殊性质：它是哈密顿群（即非阿贝尔群，但所有子群都是正规子群）。

## 15 可解群 (Solvable Groups)

## 15.1 背景：伽罗瓦理论

设  $f(t) \in \mathbb{Q}[t]$ , 令  $L$  为  $f$  在  $\mathbb{Q}$  上的分裂域,  $G = \text{Gal}(L/\mathbb{Q})$  为伽罗瓦群。核心定理如下:

$$f \text{ 有根式解} \iff G \text{ 是可解群}$$

## 15.2 定义：导子列与可解性

定义 15.1 (导子列 Derived Series). 设  $G$  为群, 定义其导子列如下:

- $D^0(G) = G^{(0)} = G$
- $D^1(G) = G^{(1)} = [G, G] = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle$  (换位子群)
- $D^n(G) = G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$

定义 15.2 (可解群). 若存在整数  $n$  使得  $G^{(n)} = \{1\}$ , 则称  $G$  为可解群。

## 15.3 基本性质与例子

- Abel 群:  $G^{(1)} = \{1\}$ , 故必然可解。
- 低阶对称群:  $S_2, S_3, S_4$  均为可解群。
  - $S_3^{(1)} = A_3 \cong C_3, S_3^{(2)} = \{1\}$ 。
  - $S_4^{(1)} = A_4, S_4^{(2)} = V_4$  (Klein 四元群),  $S_4^{(3)} = \{1\}$ 。
- 重要结论:  $S_n (n \geq 5)$  不可解 (因为  $A_n$  为非 Abel 单群)。

## 补充：关于商群（同态像）可解性的详细证明

命题 15.3 (同态像的可解性). 设  $G$  是可解群,  $\phi: G \rightarrow H$  是满同态。则  $H$  (即  $G$  的同态像) 也是可解群。

特例: 若  $N \trianglelefteq G$ , 取自然同态  $\pi: G \rightarrow G/N$ , 则商群  $G/N$  是可解群。

证明. 证明的核心在于建立原群导子列与像群导子列之间的关系。

第一步: 建立引理

我们要证明对于任意  $k \geq 0$ , 有:

$$\phi(G^{(k)}) = H^{(k)}$$

归纳法证明：

1. 奠基 ( $k = 0$ ):

$$\phi(G^{(0)}) = \phi(G) = H = H^{(0)}$$

显然成立。

2. 归纳 ( $k = 1$ ): 回顾换位子映射性质:  $\phi([x, y]) = [\phi(x), \phi(y)]$ 。

$$\phi(G^{(1)}) = \phi(\langle [x, y] \rangle) = \langle [\phi(x), \phi(y)] \rangle = [H, H] = H^{(1)}$$

3. 递推 ( $k \rightarrow k + 1$ ): 假设  $\phi(G^{(k)}) = H^{(k)}$  成立。

$$\begin{aligned}\phi(G^{(k+1)}) &= \phi([G^{(k)}, G^{(k)}]) \\ &= [\phi(G^{(k)}), \phi(G^{(k)})] \quad (\text{同态保持换位子结构}) \\ &= [H^{(k)}, H^{(k)}] \quad (\text{利用归纳假设}) \\ &= H^{(k+1)}\end{aligned}$$

至此，引理  $\phi(G^{(k)}) = H^{(k)}$  得证。

**第二步：利用  $G$  的可解性**

因为  $G$  是可解群，根据定义，存在某个整数  $n$  使得导子列收缩到单位元：

$$G^{(n)} = \{e_G\}$$

**第三步：推导  $H$  的可解性**

对  $G^{(n)}$  应用同态  $\phi$ ：

$$\begin{aligned}H^{(n)} &= \phi(G^{(n)}) \quad (\text{根据第一步引理}) \\ &= \phi(\{e_G\}) \\ &= \{e_H\} \quad (\text{同态将单位元映射为单位元})\end{aligned}$$

结论： $H$  的导子列在第  $n$  步也收缩到了单位元  $\{e_H\}$ 。因此， $H$  是可解群。  $\square$

**直观理解：直观理解：投影仪原理**

可以将满同态  $\phi$  想象成一台投影仪，把  $G$  投影成了  $H$ 。

- 上述证明告诉我们：如果你在  $G$  内部进行“取换位子”的操作，然后把结果投影下来；这就完全等同于你先投影下来，然后在  $H$  内部进行同样的“取换位子”操作。

- 既然原物体  $G$  最终能通过这种操作“消融”成单点（单位元），那么它的影子  $H$  自然也会随之“消融”。

**推论 15.4** (等价定义).  $G$  是可解群当且仅当存在有限长的正规子群列:

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$$

使得每个商群因子  $H_i/H_{i-1}$  都是 **Abel 群**。

**证明：可解群的等价定义.** 我们需要证明  $G$  可解  $\iff$  存在正规列  $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$  且商群均为 Abel 群。

**1. 必要性 ( $\implies$ ):** 假设  $G$  是可解群。根据定义, 存在  $n$  使得导子列  $G^{(n)} = \{1\}$ 。我们可以直接构造这个正规列, 取  $H_i$  为导子列的“倒序”: 设  $r = n$ , 令  $H_i = G^{(n-i)}$ 。则序列变为:

$$\{1\} = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

此时, 第  $i$  个商群因子为:

$$H_i/H_{i-1} = G^{(n-i)}/G^{(n-i+1)} = G^{(k)}/G^{(k+1)} \quad (\text{令 } k = n - i)$$

回顾导子群定义  $G^{(k+1)} = [G^{(k)}, G^{(k)}]$ 。我们知道, 任何群模掉其换位子群, 得到的商群必然是 Abel 群 (交换群)。因此, 构造的序列满足所有条件。

**2. 充分性 ( $\impliedby$ ):** 假设存在正规列  $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$ , 且每个商群  $H_i/H_{i-1}$  都是 Abel 群。我们需要证明  $G$  的导子列最终收缩为  $\{1\}$ 。我们将证明导子列“收缩得比  $H$  序列快”。

归纳法证明:

- **第 1 步:** 考虑  $G^{(1)} = [G, G] = [H_r, H_r]$ 。因为商群  $H_r/H_{r-1}$  是 Abel 群, 意味着  $H_r$  中任意元素的换位子都落在  $H_{r-1}$  中 (即换位子在模  $H_{r-1}$  后为单位元)。

$$\implies G^{(1)} \subseteq H_{r-1}$$

- **第 2 步:** 考虑  $G^{(2)} = [G^{(1)}, G^{(1)}]$ 。由上一步知  $G^{(1)} \subseteq H_{r-1}$ , 故  $G^{(2)} \subseteq [H_{r-1}, H_{r-1}]$ 。同理, 因为  $H_{r-1}/H_{r-2}$  是 Abel 群, 故其换位子群包含在  $H_{r-2}$  中。

$$\implies G^{(2)} \subseteq H_{r-2}$$

- **第  $k$  步:** 利用归纳法可得  $G^{(k)} \subseteq H_{r-k}$ 。



当  $k = r$  时，我们有：

$$G^{(r)} \subseteq H_{r-r} = H_0 = \{1\}$$

即  $G^{(r)} = \{1\}$ 。根据定义， $G$  是可解群。 □

**直观理解：直观理解：为什么 Abel 商群意味着“收缩”？**

条件“ $H_i/H_{i-1}$  是 Abel 群”本质上是在说： $H_i$  的换位子群被“压缩”进了下一层  $H_{i-1}$ 。

- 如果商群是 Abel 的，说明  $xyH_{i-1} = yxH_{i-1}$ 。
- 这等价于  $xyx^{-1}y^{-1} \in H_{i-1}$ 。
- 也就是说，每做一次“求导（取换位子）”操作，我们就至少能往在这个梯子上“下”一级。梯子是有限的，所以最终一定会掉到底端  $\{1\}$ 。

## 15.4 实例详解：上三角矩阵群 $T_n(k)$

上三角矩阵群是群论中验证可解性的经典模型。通过它，我们可以清晰地看到群结构是如何通过“层级”被拆解为简单的 Abel 群的。

### 15.4.1 定义与符号

设  $k$  为一个域。

1. **上三角群  $T_n(k)$** ：包含所有行列式非零的上三角矩阵。

$$T_n(k) = \{(a_{ij}) \in GL_n(k) \mid a_{ij} = 0 \text{ 若 } i > j\}$$

2. **单位上三角群系列  $U_{n,m}(k)$** ：定义  $U_{n,m}(k)$  为对角线元素为 1，且对角线往上数的  $m-1$  条斜线均为 0 的矩阵集合。数学定义：

$$U_{n,m}(k) = \{(a_{ij}) \in T_n(k) \mid a_{ii} = 1, \text{ 且 } a_{ij} = 0 \text{ 若 } 0 < j - i < m\}$$

**直观层级：**

- $U_{n,1}(k)$ ：即标准的单位上三角群（对角线为 1，上方任意）。
- $U_{n,2}(k)$ ：对角线为 1，且紧邻的第一条超对角线全为 0。
- $U_{n,n}(k)$ ：全为 0（除了对角线），即单位矩阵  $\{I\}$ 。

### 15.4.2 证明：利用正规列证明可解性

我们构造如下的正规子群列：

$$T_n(k) \supseteq U_{n,1}(k) \supseteq U_{n,2}(k) \supseteq \cdots \supseteq U_{n,n-1}(k) \supseteq \{I\}$$

为了证明  $T_n(k)$  可解，我们需要证明该序列中每一层的商群都是 Abel 群。

**步骤 1：第一层商群** 考虑映射  $\psi : T_n(k) \rightarrow (k^\times)^n$ （对角矩阵群），定义为提取对角线元素：

$$\psi(A) = (a_{11}, a_{22}, \dots, a_{nn})$$

- 这是一个群满同态（上三角矩阵乘积的对角线等于对角线的乘积）。
- 其核  $\text{Ker}(\psi)$  正是对角线全为 1 的矩阵，即  $U_{n,1}(k)$ 。
- 根据同构定理： $T_n(k)/U_{n,1}(k) \cong (k^\times)^n$ 。
- $(k^\times)^n$  是对角矩阵乘法群，显然是 **Abel 群**。

**步骤 2：后续层商群（关键难点）** 对于  $i \geq 1$ ，我们要证明  $U_{n,i}(k)/U_{n,i+1}(k)$  是 Abel 群。

**分析结构：** $U_{n,i}(k)$  中的矩阵  $A$  可以写成  $A = I + X$ ，其中  $X$  的非零元素只能出现在第  $i$  条超对角线及更上方。

$$A = \begin{pmatrix} 1 & \cdots & 0 & * & \cdots \\ & 1 & \cdots & 0 & * \\ & & \ddots & & 0 \\ & & & 1 & \cdots \\ 0 & & & & 1 \end{pmatrix}$$

**构造同态：**定义映射  $\phi_i : U_{n,i}(k) \rightarrow k^{n-i}$ （向量加法群），提取第  $i$  条超对角线上的元素：

$$\phi_i(A) = (a_{1,1+i}, a_{2,2+i}, \dots, a_{n-i,n})$$

**验证同态性质：**设  $A, B \in U_{n,i}(k)$ 。写成  $A = I + D_A + E_A$ ，其中  $D_A$  仅包含第  $i$  条超对角线元素， $E_A$  为更高阶项（第  $i+1$  条及以上）。计算乘积：

$$\begin{aligned} AB &= (I + D_A + E_A)(I + D_B + E_B) \\ &= I + (D_A + D_B) + (E_A + E_B) + \underbrace{D_A D_B + D_A E_B + \cdots}_{\text{更高阶项}} \end{aligned}$$

注意交叉项  $D_A D_B$ ：矩阵乘法会导致非零元素向右上方平移。 $D_A$  偏移  $i$  格， $D_B$  偏移  $i$  格，故  $D_A D_B$  偏移  $2i$  格。因为  $i \geq 1$ ，所以  $2i \geq i+1$ 。这意味着所有乘积交叉项都落入了  $U_{n,i+1}$  的范围内（更高阶）。因此，在第  $i$  条超对角线上，元素的运算法则退化为简单的加法：

$$\phi_i(AB) = \phi_i(A) + \phi_i(B)$$

结论：

- $\phi_i$  是从乘法群到加法群的同态。
- $\text{Ker}(\phi_i)$  是第  $i$  条超对角线也为 0 的矩阵，即  $U_{n,i+1}(k)$ 。
- 商群  $U_{n,i}/U_{n,i+1} \cong k^{n-i}$ （向量空间加法群），是 **Abel 群**。

综上所述， $T_n(k)$  的所有商群因子均为 Abel 群，故  $T_n(k)$  是可解群。

#### 15.4.3 另一种视角：导子列的指数级收缩

如果直接计算导子列，我们会发现收敛速度极快。

**直观理解：矩阵乘法的“移位”与换位子的“消去”**

设  $X, Y$  为严格上三角矩阵，其非零元素起始于第  $m$  条超对角线。

1. 乘积移位： $XY$  的非零元素将起始于第  $2m$  条超对角线（因为位移叠加）。
2. 换位子抵消：

$$[I + X, I + Y] \approx (I + X + Y + XY)(I - X - Y + XY) \approx I + (XY - YX)$$

线性项  $X, Y$  被抵消，只剩下二次项。

**结论：**若  $A, B \in U_{n,m}$ ，则  $[A, B] \in U_{n,2m}$ 。即零的宽度从  $m$  翻倍到  $2m$ 。

由此可得导子列的包含关系：

$$T_n^{(1)} = U_{n,1}, \quad T_n^{(2)} \subseteq U_{n,2}, \quad T_n^{(3)} \subseteq U_{n,4}, \quad \dots, \quad T_n^{(k)} \subseteq U_{n,2^{k-1}}$$

只要  $2^{k-1} \geq n$ ，导子列就收缩为  $\{I\}$ 。

#### 15.4.4 具体例子： $n = 3$ 的情形

为了形象理解，我们列出  $T_3(k)$  的结构：

第 0 层  $T_3(k)$ :

$$\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$$

第 1 层  $U_{3,1}(k) = T_3^{(1)}$ : (对角线变为 1)

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

商群  $T_3/U_{3,1} \cong k^\times \times k^\times \times k^\times$  (对角元乘法)。

第 2 层  $U_{3,2}(k)$ : (第 1 条超对角线  $a, c$  变为 0)

$$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

商群  $U_{3,1}/U_{3,2} \cong k \times k$  (对应元素  $a, c$  的加法)。

第 3 层  $U_{3,3}(k) = \{I\}$ : (第 2 条超对角线  $b$  变为 0)

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

商群  $U_{3,2}/\{I\} \cong k$  (对应元素  $b$  的加法)。

整个过程就像是“剥洋葱”，先剥掉对角线，再一层一层剥掉上面的斜线，每一层剥下来的皮都是平坦的 (Abel 的)。

## 16 幂零群 (Nilpotent Groups)

### 16.1 定义：下中心列

定义 16.1 (下中心列 Lower Central Series). 定义  $G$  的下中心列为：

- $G^1 = C^1(G) = [G, G]$
- $G^r = C^r(G) = [G, C^{r-1}(G)]$

若存在  $r$  使得  $G^r = \{1\}$ ，则称  $G$  为幂零群。

### 直观理解：收缩速度对比

- 导子列 (可解):  $[H, H]$  (强强对抗), 收缩快。
- 下中心列 (幂零):  $[G, H]$  (强弱对抗), 收缩慢。
- 因此: 幂零群  $\implies$  可解群, 反之不成立。

## 16.2 等价定义：上中心列

定义上中心列  $Z_n(G)$ :

$$Z_0(G) = 1, \quad Z_1(G) = Z(G), \quad Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$$

命题:  $G$  是幂零群  $\iff$  存在  $r$  使得  $Z_r(G) = G$ 。

### 深入解析：上下中心列的对偶性与直观理解

在幂零群的理论中, 下中心列  $(G^k)$  和上中心列  $(Z_k)$  具有完美的对偶性。理解这种对偶性是掌握幂零群结构的关键。

**1. 核心联系：换位子定义** 笔记中给出的上中心列递归定义是  $Z_{k+1}/Z_k = Z(G/Z_k)$ 。这个定义虽然代数上简洁, 但在计算时不直观。我们需要证明它等价于:

$$[G, Z_{k+1}] \subseteq Z_k$$

**推导证明.** 设  $x$  是群  $G$  中的一个元素, 且  $Z_k$  是  $G$  的一个正规子群。我们来解析  $x \in Z_{k+1}$  的含义:

1. **根据定义:**  $x \in Z_{k+1}$  当且仅当  $x$  在商群  $G/Z_k$  中的像  $\bar{x} = xZ_k$  属于商群的中心  $Z(G/Z_k)$ 。
2. **翻译为交换律:**  $\bar{x}$  在中心里, 意味着它与商群中任意元素  $\bar{g} = gZ_k$  均可交换:

$$(xZ_k)(gZ_k) = (gZ_k)(xZ_k), \quad \forall g \in G$$

3. **利用陪集运算:** 根据商群乘法规则, 上式等价于:

$$(xg)Z_k = (gx)Z_k$$

4. 利用陪集相等条件：两个陪集  $aH = bH$  相等，当且仅当  $ab^{-1} \in H$ 。此处  $H = Z_k$ 。

$$(xg)(gx)^{-1} \in Z_k$$

5. 展开计算：

$$xgx^{-1}g^{-1} \in Z_k$$

注意：虽然这通常记为  $[x^{-1}, g^{-1}]$ ，但由于  $Z_k$  是正规子群，包含逆元和共轭，这完全等价于  $[g, x] \in Z_k$ 。我们也可以直接验证  $ab^{-1} \in H \iff a \in Hb \iff b^{-1}a \in H$ 。更直接地， $(gx)Z_k = (xg)Z_k \iff (gx)(xg)^{-1} \in Z_k \iff g x g^{-1} x^{-1} \in Z_k$ 。即：

$$[g, x] \in Z_k$$

结论： $Z_{k+1}$  是所有满足“与  $G$  中任意元素换位后落入  $Z_k$ ”的元素集合。即  $[G, Z_{k+1}] \subseteq Z_k$ 。□

命题 16.2 (上下中心列的等价性). 设  $G$  是群。若  $G$  的下中心列在第  $r$  步终止于  $\{1\}$  (即  $G^r = \{1\}$ )，则其上中心列在第  $r$  步必然到达  $G$  (即  $Z_r = G$ )，反之亦然。且最小的这样的  $r$  (幂零类) 是相同的。

证明：利用包含关系。我们通过证明以下包含关系来建立两者联系：

$$G^i \subseteq Z_{r-i+1} \implies G \text{ 幂零}$$

方向 ( $\implies$ )：假设  $G^r = \{1\}$ 。利用归纳法证明  $G^k \subseteq Z_{r-k+1}$ 。

- 当  $k = r$  时： $G^r = \{1\} = Z_0$  (注意：这里记  $Z_0 = 1$ )。实际上应对应上中心列定义的下标，更精确的归纳是证明  $G^k \subseteq Z_{r-k}$  (如果从 0 开始计数)。

- 让我们使用更直观的“步数”归纳：

1. 第 1 步：因为  $G^r = [G, G^{r-1}] = \{1\}$ ，这意味着  $G^{r-1}$  中的元素与  $G$  换位后均为 1。根据中心定义，这意味着  $G^{r-1} \subseteq Z(G) = Z_1$ 。

2. 第 2 步：推导  $G^{r-2} \subseteq Z_2$

已知上一轮的结论  $G^{r-1} \subseteq Z_1$ 。现在我们考察  $G^{r-2}$ ：

– 下行 (定义展开)：根据下中心列的递归定义，有

$$[G, G^{r-2}] = G^{r-1}$$

– 联立 (结合条件)：将已知的  $G^{r-1} \subseteq Z_1$  代入上式，得到

$$[G, G^{r-2}] \subseteq Z_1$$

– 上行（逆向判定）：利用上中心列的等价定义

$$[G, X] \subseteq Z_k \iff X \subseteq Z_{k+1}$$

令  $k = 1, X = G^{r-2}$ ，上述包含关系直接蕴含了：

$$G^{r-2} \subseteq Z_{1+1} = Z_2$$

3. 第  $k$  步：一般地，若  $G^{r-k} \subseteq Z_k$ ，则  $[G, G^{r-k-1}] = G^{r-k} \subseteq Z_k \implies G^{r-k-1} \subseteq Z_{k+1}$ 。
4. 终点：当推导到最后一步时，我们有  $G^1 \subseteq Z_{r-1}$ ，最终  $G^0 (= G) \subseteq Z_r$ 。即  $G = Z_r$ 。

反之 ( $\Leftarrow$ ) 的证明逻辑完全相同，只是方向相反。 □

### 直观理解：直观理解：剥洋葱 vs 爬楼梯

如何形象地理解这两种序列？

#### 1. 下中心列（剥洋葱）：

- 我们拿着一把叫“换位子”的刀，不断地切掉群的外皮。
- $G \rightarrow [G, G] \rightarrow [G, [G, G]] \dots$
- 如果洋葱心是空的（单位元），那就是幂零群。

#### 2. 上中心列（爬楼梯/建筑）：

- 第 1 层 ( $Z_1$ )：绝对和平主义者。他们和任何人都不吵架 ( $[g, x] = 1$ )。
- 第 2 层 ( $Z_2$ )：温和派。他们会吵架，但吵出来的结果仅限于“绝对和平主义者” ( $[g, x] \in Z_1$ )。这意味着在模掉  $Z_1$  的世界里，他们也是和平的。
- 第 3 层 ( $Z_3$ )：次级温和派。他们吵架的结果属于  $Z_2$ 。
- 幂零群：意味着如果我们一层一层地把“和平主义者”和“相对和平主义者”收编，最后能把整个群  $G$  的人都收编进去。也就是说，这个群里没有“刺头”（无法被归类的顽固分子）。

## 16.3 性质与反例

1. 中心非平凡：若  $G$  是非平凡幂零群，则  $Z(G) \neq \{1\}$ 。
2. 封闭性：幂零群的子群、商群、直积仍为幂零群。

3. 扩张危机：幂零群的扩张不一定是幂零的。

- 反例  $S_3$ :  $1 \rightarrow A_3 \rightarrow S_3 \rightarrow C_2 \rightarrow 1$ 。虽然  $A_3, C_2$  幂零，但  $S_3$  不是幂零群（下中心列卡在  $A_3$ ）。

4. 补救（中心扩张）：若  $N \subseteq Z(G)$  且  $G/N$  幂零，则  $G$  幂零。

补充证明：为什么中心扩张能保持幂零性？

命题 16.3. 设  $N \subseteq Z(G)$  且商群  $G/N$  是幂零群，则  $G$  是幂零群。

证明. 我们利用下中心列 (Lower Central Series) 来证明。回顾下中心列定义： $G^1 = [G, G]$ ,  $G^{k+1} = [G, G^k]$ 。

第一步：利用商群的幂零性

设  $\pi: G \rightarrow G/N$  为自然同态。因为  $G/N$  是幂零群，设其幂零类为  $c$ 。这意味着  $G/N$  的下中心列在第  $c$  步收缩为商群的单位元（即集合  $N$ ）：

$$(G/N)^c = \{N\}$$

第二步：利用同态映射性质

我们知道同态保持下中心列结构，即  $\pi(G^k) = (G/N)^k$ 。将  $k = c$  代入：

$$\pi(G^c) = (G/N)^c = \{N\}$$

这意味着  $G^c$  中的所有元素在映射  $\pi$  下都变为单位元。根据同态核的定义：

$$G^c \subseteq \text{Ker}(\pi) = N$$

第三步：利用中心的“吸收”性质（关键）

现在考察  $G$  的下一步下中心列  $G^{c+1}$ ：

$$G^{c+1} = [G, G^c]$$

由于我们已经推导出  $G^c \subseteq N$ ，利用换位子的单调性：

$$[G, G^c] \subseteq [G, N]$$

此时利用已知条件  $N \subseteq Z(G)$ 。因为  $N$  在中心里，它与  $G$  中任意元素交换，即  $gng^{-1}n^{-1} = e$ 。所以：

$$[G, N] = \{1\}$$



结论:

$$G^{c+1} \subseteq \{1\} \implies G^{c+1} = \{1\}$$

$G$  的下中心列在第  $c+1$  步收缩为  $\{1\}$ , 故  $G$  是幂零群。  $\square$

### 直观理解: 直观理解: 黑洞视界

可以将中心  $Z(G)$  想象成幂零群的“黑洞视界”:

- 一般的群扩张 (如  $S_3$ ), 下中心列可能会卡在某个非平凡子群上 (如  $A_3$ ) 无法继续缩小。
- 但是, 一旦下中心列“掉”进了中心  $Z(G)$  的范围 (即  $G^c \subseteq Z(G)$ ), 它就无法逃逸了。
- 因为中心与全群的换位子直接归零 ( $[G, Z(G)] = 1$ ), 所以下一步必然直接坍塌到单位元  $\{1\}$ 。

这就是为什么“中心扩张”如此特殊且安全。

**定理 16.4** (有限  $p$ -群). 设  $|G| = p^\alpha$  ( $p$  为素数), 则  $G$  是幂零群 (从而也是可解群)。

**证明思路:** 利用归纳法。关键在于有限  $p$ -群中心  $Z(G)$  非平凡, 通过商群  $G/Z(G)$  降阶归纳, 利用中心扩张的性质得证。

### 详解: 有限 $p$ -群是幂零群的证明

**证明.** 我们对群的阶数  $|G| = p^\alpha$  进行数学归纳法。

**1. 归纳奠基** ( $\alpha = 1$ ): 当  $\alpha = 1$  时,  $|G| = p$ . 此时  $G \cong C_p$  (素数阶循环群)。循环群是 Abel 群, 而 Abel 群必然是幂零群 (其导子列和下中心列在第 1 步即归零)。结论成立。

**2. 归纳假设:** 假设对于所有阶数为  $p^k$  ( $k < m$ ) 的  $p$ -群, 结论均成立。

**3. 归纳递推** ( $|G| = p^m$ ): 设  $G$  是阶数为  $p^m$  ( $m > 1$ ) 的群。

#### • 步骤 A: 利用类方程证明中心非平凡

我们需要用到群论中的核心引理: 非平凡有限  $p$ -群的中心  $Z(G)$  非平凡。

简要理由: 回顾类方程

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

其中  $\text{sum}$  是对非中心元素共轭类的求和。因为  $G$  是  $p$ -群，非中心元素的共轭类大小  $[G : C_G(x_i)]$  必然是  $p$  的倍数（且大于 1）。同时  $|G|$  也是  $p$  的倍数。故  $p$  必须整除  $|Z(G)|$ 。这意味着  $|Z(G)| \geq p > 1$ ，即  $Z(G) \neq \{1\}$ 。

- **步骤 B：降阶 (Dimension Reduction)**

考察商群  $\bar{G} = G/Z(G)$ 。由于  $|Z(G)| \geq p$ ，商群的阶为：

$$|\bar{G}| = \frac{|G|}{|Z(G)|} \leq p^{m-1} < p^m$$

显然  $\bar{G}$  仍然是一个  $p$ -群，且阶数严格小于  $|G|$ 。

- **步骤 C：应用归纳假设**

根据归纳假设，因为  $\bar{G}$  的阶数更小，所以  $\bar{G}$  是幂零群。

- **步骤 D：应用中心扩张性质**

现在我们有：

1.  $Z(G)$  是  $G$  的中心（显然  $Z(G) \subseteq Z(G)$ ）。
2. 商群  $G/Z(G)$  是幂零群。

根据之前证明的“幂零群的中心扩张仍为幂零群”定理，我们直接得出结论： $G$  是幂零群。

□

**直观理解：直观理解：为什么  $p$ -群一定幂零？**

这个证明展示了  $p$ -群的一个美好性质：

- 它的中心  $Z(G)$  永远不会是空的（至少有  $p$  个元素）。
- 这意味着我们可以不断地把中心“剥离”出来（取商群），每次剥离群都会变小。
- 因为群是有限的，只要我们保证每次都能剥下来一点东西，最终一定能剥到只剩单位元。
- 这种“层层剥离中心”的过程，恰好对应了上中心列  $1 \rightarrow Z_1 \rightarrow Z_2 \cdots \rightarrow G$  的构造过程。

## 17 特征子群 (Characteristic Subgroups)

定义 17.1. 设  $H \leq G$ , 若对于任意自同构  $\sigma \in \text{Aut}(G)$  都有  $\sigma(H) = H$ , 则称  $H$  为  $G$  的特征子群, 记为  $H \text{ char } G$ 。

- 关系:  $H \text{ char } G \implies H \trianglelefteq G$ 。
- 传递性:  $K \text{ char } H, H \trianglelefteq G \implies K \trianglelefteq G$ 。(解决了正规子群不传递的问题)
- 例子: 中心  $Z(G)$ , 导子群  $G^{(k)}$ , 下中心列  $G^k$  均为特征子群。

## 18 单群 (Simple Groups)

单群是群论中的“原子”无法再被拆解。

### 18.1 定义

若群  $G \neq \{1\}$  且其正规子群只有  $\{1\}$  和  $G$  自身, 则称  $G$  为单群。

### 18.2 分类

1. Abel 单群: 即素数阶循环群  $C_p$ 。这是唯一可解的单群。
2. 非 Abel 单群:
  - 交错群:  $A_n$  ( $n \geq 5$ )。最小的非 Abel 单群是  $A_5$  ( $|A_5| = 60$ )。
  - 李型群: 如  $PSL_2(k)$ 。例子:  $PSL_2(\mathbb{F}_7) \cong SL_3(\mathbb{F}_2)$  (168 阶)。
  - 散在单群: 26 个例外, 如魔群 (Monster Group)。

注意 (NOTE): Thompson-Feit 定理

奇数阶群一定是可解群。这意味着所有非 Abel 单群的阶数必须是偶数。

性质	可解群 (Solvable)	幂零群 (Nilpotent)	单群 (Simple)
基本积木	Abel 群	中心 (Center)	自身不可拆
判定序列	导子列 $G^{(n)} \rightarrow 1$	下中心列 $G^n \rightarrow 1$	无非平凡正规子群
收缩速度	指数级 (翻倍)	线性 (+1)	不收缩 ( $G' = G$ )
子/商封闭	是	是	N/A
扩张封闭	是	否 (仅限中心扩张)	N/A
典型例子	$S_4, T_n(k)$	$p$ -群, $U_n(k)$	$C_p, A_5$

表 1: 群结构性质对比表

## 19 总结对比

### 19.1 核心实例：证明 $PSL_2(k)$ 是单群

本例将详细证明当域  $k$  足够大时，射影特殊线性群  $PSL_2(k)$  没有非平凡正规子群。

#### 1. 定理陈述与背景

**定理 19.1** ( $PSL_2(k)$  的单性). 设  $k$  是一个域，且  $|k| \geq 4$  (即  $k \neq \mathbb{F}_2, \mathbb{F}_3$ )。则射影特殊线性群  $PSL_2(k)$  是单群 (*Simple Group*)。

注：小域的反例

- 若  $|k| = 2$ ,  $PSL_2(\mathbb{F}_2) \cong S_3$  (非单群)。
- 若  $|k| = 3$ ,  $PSL_2(\mathbb{F}_3) \cong A_4$  (非单群)。

#### 2. 证明策略：对应定理

直接研究商群  $PSL_2(k)$  较为抽象。利用**对应定理**，我们将问题转化为  $SL_2(k)$  的结构问题。

$PSL_2(k)$  是单群  $\iff SL_2(k)$  中不存在正规子群  $N$  满足：

$$Z \subsetneq N \subsetneq SL_2(k)$$

其中  $Z = \{\pm I\}$  是中心。我们需要证明：任何包含  $Z$  且  $N \neq Z$  的正规子群  $N$ ，必然等于  $SL_2(k)$ 。

### 3. 关键工具箱

在证明前，引入两个关于  $SL_2(k)$  的代数事实（引理）：

- **引理 A (生成元)：**  $SL_2(k)$  由所有的平移矩阵  $T_{12}(\lambda)$  和  $T_{21}(\mu)$  生成。如果一个子群包含所有平移矩阵，则它等于  $SL_2(k)$ 。
- **引理 B (完美群)：** 当  $|k| > 3$  时， $SL_2(k)' = SL_2(k)$ （导群等于自身）。

### 4. 完整证明过程

**设定：** 设  $N \leq SL_2(k)$ ，且  $N \not\subseteq Z$ 。我们证明  $N = SL_2(k)$ 。

Step 1: 捕捉非平凡平移矩阵我们需要证明  $N$  中包含一个形如  $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$  ( $u \neq 0$ ) 的矩阵。

由于  $N$  包含非中心元素，必存在  $A \in N \setminus Z$ 。通过共轭变换（将  $A$  上三角化）并计算换位子  $B = [A, U]$ （其中  $U$  是特定的平移矩阵），我们可以构造出一个元素  $B \in N$ 。

经过代数讨论（排除  $a^2 = 1$  的特殊情况），总是可以在  $N$  中找到一个非零平移矩阵  $U_0 = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ 。

Step 2: 生成所有的平移矩阵已知  $U_0 \in N$ 。利用  $N$  的正规性，对任意对角矩阵  $D = \text{diag}(x, x^{-1})$ ，有：

$$DU_0D^{-1} = \begin{pmatrix} 1 & x^2u \\ 0 & 1 \end{pmatrix} \in N$$

这表明  $N$  包含集合  $\{x^2u \mid x \in k^\times\}$ 。

利用平方差恒等式  $y = (\frac{y+1}{2})^2 - (\frac{y-1}{2})^2$ ，可知  $\{x^2\}$  的加法组合可以生成整个域  $k$ 。因此， $N$  包含所有的上三角平移矩阵  $T_{12}(\lambda), \forall \lambda \in k$ 。

Step 3: 收网同理，利用外尔元素  $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  的共轭作用，可以将上三角平移矩阵转化为下三角平移矩阵  $T_{21}(\mu)$ 。

**结论：**  $N$  包含所有的平移矩阵。由引理 A 可知， $N$  包含了  $SL_2(k)$  的所有生成元。

$$\therefore N = SL_2(k)$$

这证明了  $PSL_2(k)$  是单群。 □