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 11 月 27 日

目录

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 $G_1, \ldots, G_n$，其直积定义为集合 $G_1 \times \cdots \times G_n$ 配上分量运算：

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

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

$$G = H_1 \oplus \cdots \oplus H_n$$

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 ($\Longleftarrow$) 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 ($\Longrightarrow$) 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 *($d_1 \mid d_2 \ldots$)*	***CRT*** 逻辑
$C_8 \oplus C_9$	$\cong C_{72}$	$8 \times 9 = 72$
$C_4 \oplus C_2 \oplus C_9$	$\cong C_2 \oplus C_{36}$	$C_2 \oplus (C_4 \times C_9)$
$C_2 \oplus C_2 \oplus C_2 \oplus C_9$	$\cong C_2 \oplus C_2 \oplus C_{18}$	$C_2^2 \oplus (C_2 \times C_9)$
$C_8 \oplus C_3 \oplus C_3$	$\cong C_3 \oplus C_{24}$	$C_3 \oplus (C_8 \times C_3)$
$C_4 \oplus C_2 \oplus C_3 \oplus C_3$	$\cong C_6 \oplus C_{12}$	$(C_2 \times C_3) \oplus (C_4 \times C_3)$
$C_2^3 \oplus C_3^2$	$\cong C_2 \oplus C_6 \oplus C_6$	$C_2 \oplus (C_2C_3) \oplus (C_2C_3)$

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，$nx = 0$。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 $G = P_1 + P_2 + \cdots + P_k$。

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 $G \cong P_1 \oplus \cdots \oplus P_k$。 $\square$

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 $p_1, p_2, \ldots, p_k$。

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	$p_1^{\alpha_1}$	$p_1^{\alpha_2}$	$\cdots$	$p_1^{\alpha_r}$
p_2	$p_2^{\beta_1}$	$p_2^{\beta_2}$	$\cdots$	$p_2^{\beta_r}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
p_k	$p_k^{\gamma_1}$	$p_k^{\gamma_2}$	$\cdots$	$p_k^{\gamma_r}$

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

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：*

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

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**：$PGL_n(k) \cong \mathrm{GL}_n(k)/k^\times$。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)。
- $\mathrm{GL}_n(k)/\mathrm{SL}_n(k) \cong k^\times$ (行列式映射)。
- $O(n)/\mathrm{SO}(n) \cong C_2$。

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 $\Phi : G \to G'$ 是群同态，$N \trianglelefteq G$。若 $N \subseteq \ker(\Phi)$，则存在 ** 唯一 ** 的同态 $\overline{\Phi} : G/N \to G'$ 使得 $\overline{\Phi} \circ \pi = \Phi$。

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

证明. **1. 定义：** $\overline{\Phi}(aN) = \Phi(a)$。**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 π 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 $\overline{\Phi}$ 是一个同构：

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

直观理解：直观理解

任何同态都可以分解为：商映射（压缩）$\to$ 同构映射（一一对应）$\to$ 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 $\Phi : G \to G'$ 是一个群同态，其核为 $K = \ker(\Phi)$。则映射

$$\overline{\Phi} : G/K \to \operatorname{Im}(\Phi)$$

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

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

证明. 我们需要验证 $\overline{\Phi}$ 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 $\overline{\Phi}$ 是良定的群同态。

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

- 取任意 $y \in \operatorname{Im}(\Phi)$。

- 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 $\overline{\Phi}(gK) = \Phi(g) = y$。
- 因此，$\overline{\Phi}$ 是满射。

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

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

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

结论：由于 $\overline{\Phi}$ 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 Φ 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 Φ 都被“压缩”到了 G' 中的同一个点 $\Phi(g)$ 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 $\mathrm{Im}(\Phi)$ 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**：$\pi_{n,d} : \mathbb{Z}_n \to \mathbb{Z}_d$，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：

$$\overline{\pi} : G/N_0 \to G/H, \quad aN_0 \mapsto aH$$

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：

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

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

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 $\mathrm{sgn}: S_n \to \{1, -1\}$。我们知道 $A_n = \ker(\mathrm{sgn})$。对于任意换位子 $x = aba^{-1}b^{-1}$，应用同态性质：

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

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 $(\mathrm{GL}_n(k))^{(1)} = \mathrm{SL}_n(k)$。

证明. 同样证明双向包含。

1. 证明 $\mathrm{GL}_n' \subseteq \mathrm{SL}_n$ 利用行列式同态 $\det: \mathrm{GL}_n(k) \to k^\times$。我们知道 $\mathrm{SL}_n(k) = \ker(\det)$。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 $\mathrm{SL}_n(k)$ 中，故 $\mathrm{GL}_n' \subseteq \mathrm{SL}_n$。

2. 证明 $\mathrm{SL}_n \subseteq \mathrm{GL}_n'$ 线性代数告诉我们，$\mathrm{SL}_n(k)$ 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 $\mathrm{GL}_n(k)$ 中的换位子。

取对角矩阵 $D = \mathrm{diag}(u, 1, \dots, 1) \in \mathrm{GL}_n(k)$ 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： $\mathrm{GL}_n'=\mathrm{SL}_n$。 □

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 $\forall\sigma\in\mathrm{Aut}(G),\sigma(H)=H$，则称 H 为 G 的特征子群，记作 $H\ char\ G$。*

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. $H_0\ char\ H_1, H_1\trianglelefteq G\implies H_0\trianglelefteq G$。

2. $H_0\ char\ H_1, H_1\ char\ G\implies H_0\ char\ G$。

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：** $H_0\ char\ H_1, H_1\trianglelefteq G\implies H_0\trianglelefteq G$。

2. **完全传递性：** $H_0\ char\ H_1, H_1\ char\ G\implies H_0\ char\ G$。

证明性质 1：$H_0\ char\ H_1, H_1\trianglelefteq G\implies H_0\trianglelefteq G$. 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）$\phi_g:G\to G$，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 ϕ_g 限制在 H_1 上，得到映射：

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

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

3. 利用特征子群定义已知 H_0 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 *char* H_1, H_1 *char* $G \implies H_0$ *char* G. 我们要证明对于 G 的任意自同构 $\sigma \in \mathrm{Aut}(G)$，都有 $\sigma(H_0) = H_0$。

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

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

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

2. 第二层限制 (H_0 的不变性) 因为 H_0 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 σ 是任意选取的，故 H_0 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 ϕ_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：$H_0 \trianglelefteq H_1 \trianglelefteq G \nRightarrow H_0 \trianglelefteq G$。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 $G_1, \ldots, G_r$，其直积 $(g_1, \ldots, g_r)$ 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 $N_1 \times \cdots \times N_r$ 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 $\phi_i : H \to G_i$，存在 ** 唯一 ** 的同态 $\Phi : H \to P$ 使得 $\pi_i \circ \Phi = \phi_i$。

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

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。