

# Group and Galois theory - Midterm Revision

冯熙喆

2025 年 11 月 12 日

## Tips

在相关习题上遇到困难的时候, 最好的做法是检查自己是否已经实现了这个群, 而不是直接查看答案。

1.

就是所有阶整除  $n$  的循环群。

2.

假设  $G$  不是有限群。由题意, 它的循环子群是有限的, 假设我们已经取出了所有两两不等的循环子群  $\{\langle g_1 \rangle, \langle g_2 \rangle \cdots \langle g_r \rangle\}$ , 我们知道这些循环子群都是有限群 (否则存在一个循环子群有无限个循环子群), 因为这些有限循环子群个数是有限的, 总存在  $g_{r+1} \in G$  不属于上述的任何一个子群。显然它能够生成一个循环子群。这个子群不是上述任意循环子群之一。这便导出了矛盾。

**Remark:** 这个命题对可数的情形也是成立的, 但是逆命题对于可数的情形不成立 (一个阶数可数的群可能有不可数个子群)。

3.

$\text{Ker} = Z(G)$  的证明是平凡的, 这就是中心的定义。

$\text{Im}$  的正规性可以这样验证: 任给  $g$ ,  $\phi \text{Int}(g) \phi^{-1} = \text{Int}(\phi(g))$ 。

4.

任取  $g, n$ ,  $(gng^{-1}n^{-1}) \in \text{Ker}\phi \Rightarrow (gng^{-1}) \in N$ 。

5.

任意给定  $n \in N \cap K, k \in K$ ,  $knk^{-1}$  仍然属于  $N$ , 也仍然属于  $K$ 。

考虑自然的同态  $K \rightarrow KN/N$ ,  $k \mapsto kN$ , 它的核自然就是  $K \cap N$ 。任取  $KN/N$  中的元素, 它都形如  $k_iN$ , 所以它显然成为某个元素的像, 因此这个同态是满射。

据同态第一定理就得到了证明。

6.

$\Rightarrow$  利用  $(hk)^{-1} = k^{-1}h^{-1} \in KH$  可得  $HK \subset KH$ ,  $kh = (h^{-1}k^{-1})^{-1} \in HK$ , 那么  $KH \subset HK$ , 得证。

$\Leftarrow$  只要验证封闭性, 这是显然的。

7.

$H \cap K$  是  $H$  的子群, 考虑左陪集  $\{h_1(H \cap K), h_2(H \cap K), \dots, h_n(H \cap K)\}$ , 集合的大小自然是  $H/(H \cap K)$ , 不难证明  $h_1K, h_2K, \dots, h_nK$  的两两不交且并成了  $HK$ 。从而命题的计数成立。

8.

显然  $H \cap K < H$ 。

由 (7) 的论证我们知道, 如果  $h_i(H \cap K) \neq h_j(H \cap K)$ , 那么  $h_iK \neq h_jK$ , 因此如果  $\Lambda$  是一个指标集, 使得  $\{h_\lambda\}_{\lambda \in \Lambda}$ , 那么  $\{h_\lambda K\}_{\lambda \in \Lambda}$  一定是  $G$  中两两不等的左陪集。因此  $[H : H \cap K] [G : K]$ 。

指标有限的情况下, 如果等号成立,  $\Lambda$  的大小就是  $[G : K]$ , 可以知道  $\{h_\lambda K\}_{\lambda \in \Lambda}$  就是  $G$  关于  $K$  的一个陪集分解, 因此  $G = HK$ , 又因为  $HK$  已经构成一个群, 就可以知道  $HK = KH$ , 因此命题正向成立。

下面说明命题逆向成立: 如果  $G = KH$ , 那么就有  $HK = KH = G$ , 它们都是群,  $\{h_\lambda K\}_{\lambda \in \Lambda}$  是  $HK$  的一个陪集分解, 自然它也是  $G$  的一个陪集分解。同时  $\{h_\lambda H \cap K\}_{\lambda \in \Lambda}$

又给出了  $H$  的陪集分解, 从而两个指标相等 (均为  $\Lambda$  的大小)。

9.

由 (7),(8) 可知  $H \cap K$  是  $H$  的有限指标子群。显然如果  $\{g_\alpha H\}_{\alpha \in A}$  是  $H$  在  $G$  中的左陪集,  $\{h_\beta(H \cap K)\}_{\beta \in B}$  是  $H \cap K$  在  $H$  中的左陪集, 那么

$$\bigcup_{\alpha \in A, \beta \in B} g_\alpha h_\beta (H \cap K) = G$$

因此  $(H \cap K)$  在  $G$  中的左陪集包含于  $\{g_\alpha h_\beta (H \cap K)\}_{\alpha \in A, \beta \in B}$  之中, 进而我们就得到了  $[G : H \cap K] \leq [G : H][H : H \cap K] \leq [G : H][G : K]$ 。

如果  $G \neq KH$ , 那么第二个不等号不能取等, 因此只需要验证  $G = KH$  的情况能够取等。此时, 我们可以改写  $H$  在  $G$  中的左陪集为  $\{k_\alpha H\}_{\alpha \in A}$  ( $k_\alpha \in K$ ), 完全类似地, 我们可以得出, 如果  $k_1 h_1 H \cap K = k_2 h_2 H \cap K$ , 那么  $k_1 k_2^{-1}, h_1 h_2^{-1} \in H \cap K$ , 因此确实能够取等。

10.

假设  $\mathfrak{S}_n$  有一个非平凡正规子群  $N$ , 那么  $\mathfrak{A}_n \cap N$  也是一个正规子群。

如果  $N$  之中的偶置换有且仅有  $\{1_{\mathfrak{S}_n}\}$ , 那么它里面的任意两个非单位元素的乘积是一个偶置换, 因此它们互为逆元, 进一步, 这个群至多 2 个元素, 这样的非平凡正规子群不存在。因此  $N$  之中必有非平凡的偶置换。

利用  $N$  中有非  $1_{\mathfrak{S}_n}$  偶置换这一性质,  $\mathfrak{A}_n \cap N$  是  $\mathfrak{A}_n$  的一个非平凡正规子群, 据  $\mathfrak{A}_n$  的单性可以得出  $\mathfrak{A}_n \cap N = \mathfrak{A}_n$ , 且  $\mathfrak{S}_n$  没有比  $\mathfrak{A}_n$  更大的子群, 因此  $N$  只能是  $\mathfrak{A}_n$ 。

11.

先证明这确实是一个同态, 乘法交换律给出了

$$\prod_{1 \leq i < j \leq n} \frac{\tau(i) - \tau(j)}{i - j} \frac{\sigma(i) - \sigma(j)}{i - j} = \prod_{1 \leq i < j \leq n} \frac{\tau(\sigma(i)) - \tau(\sigma(j))}{\sigma(i) - \sigma(j)} \frac{\sigma(i) - \sigma(j)}{i - j}$$

因此确实是同态。再证明在生成元上面符号映射是一致的, 所以它就是之前的符号映射。

12.

利用陪集分解将  $G$  中的元素表示为  $g^k z$  (表示不必唯一), 就可以得到交换性。

13.

$\Rightarrow$  这由双传递性的定义保证。

$\Leftarrow$  若这样的集合存在, 那么我们可以将  $(g, g') \notin \Delta$  映射到任意  $(g, g'') \notin \Delta$ 。考虑到  $\text{Stab}(x'')$  也传递地作用于  $X - \{x''\}$ , 可以将它映射到任意  $X \times X - \Delta$  中的元素  $(g''', g'')$ , 这就满足了双传递性的定义。

#### 14. Jordan 的定理

考虑对集合  $S := \{(g, x) \mid gx = x\}$  进行计数, 如果原命题不成立, 那么每一个  $g_i$  至少带来集合中的一个元素, 且  $\forall x, (1_G, x) \in S$ , 因此集合的大小大于  $|G|$ 。然而对  $x$  计数, 我们知道  $|\text{Stab}(x)| = |G|/|X|$ , 且  $\text{Stab}(x)$  两两共轭, 大小相等, 可以得出  $|S| = |G|$ 。这导出了矛盾。

#### 15. Ore 的定理

我们利用前面的命题来证明: 在左诱导表示里面,  $H$  包含了表示的核  $\text{Ker}\tau \subseteq H$ , 据此我们希望证明:  $H$  就是  $\text{Ker}\tau$ :

因为  $|\text{Im}\tau| = |G : \text{Ker}\tau| = |G : H| |H : \text{Ker}\tau| = p |H : \text{Ker}\tau|$ , 我们得到  $\text{Im}\tau$  之中包含素因子  $p$ , 因此  $\text{Im}\tau$  作为  $\mathfrak{S}_p$  的子群只能是  $p$  阶群 (否则  $|G|$  有更小的素因子)。这就是说  $|H : \text{Ker}\tau| = 1$ , 即  $H = \text{Ker}\tau \triangleleft G$ 。

16.

我们知道  $GL(2; \mathbb{F}_p)$  中有  $(p^2 - 1)(p^2 - p)$  个元素, 从而它的 Sylow- $p$  子群的阶数是  $p$  (它是一个循环群), 个数应该整除  $(p^2 - 1)(p^2 - p)$  且模  $p$  余 1。那么 Sylow  $p$ -子群的个数可能是  $1, p+1, np+1 (n \geq 2)$ 。下面证明个数只能是  $p+1$ 。这个子群作为一般线性群的子群, Sylow  $p$ -子群至少包括如下两个:

$U_1 = \{g \mid g \text{ 是对角元素为 } 1 \text{ 的上三角矩阵}\},$

$L_1 = \{g \mid g \text{ 是对角元素为 } 1 \text{ 的下三角矩阵}\},$  因此 Sylow- $p$  子群至少有两个。

下面我们证明这样的 Sylow  $p$ -子群的个数不多于  $p + 1$  个：任给 Sylow  $p$ -子群  $H = \langle h \rangle$ ，那么  $h$  在  $\mathbb{F}_p[X]$  之中适合多项式方程  $X^p - 1 = 0$ ，这个方程同时等价于  $(X - 1)^p = 0$ ，因此作为线性算子的  $h$  必然只有特征值 1，且特征值 1 的特征子空间一定是一个线性真子空间（那么这个空间应当是 1 维的）。下面我们建立 Sylow  $p$ -子群之集  $S$  到  $\mathbb{P}\mathbb{F}_p^2$  之间的映射

$$f : S \rightarrow \mathbb{P}\mathbb{F}_p^2, \langle h \rangle \mapsto \text{Ker}(h - 1)$$

下面证明这个映射是 Well-defined 的，我们需要说明任意  $\langle h \rangle$  以及  $h_1, h_2 \in \langle h \rangle$ ，总有  $\text{Ker}(h_1 - 1) = \text{Ker}(h_2 - 1)$ ，这是显然的，因为两个元素互为对方的幂次。

再证明这个映射是一个单射：如果两个  $p$  阶元素  $h_1, h_2$  有着相同的特征空间，那么他们属于同一个群。

考虑  $\text{Stab}(\text{span}\{e_1\})$  中  $p$  阶元素的性质：

这样的矩阵一定形如  $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ ，它的  $p$  次方的对角元素是 1 和  $d^p = 1$ （注意要区分群乘法和矩阵的乘法），利用数论的知识我们知道  $d$  只能为 1，这就是说明  $\text{Stab}(\text{span}\{e_1\})$  中的  $p$  阶元素都形如  $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ ，也就是说  $\text{Stab}(\text{span}\{e_1\})$  中  $p$  阶子群是唯一的，就说明了有着相同特征空间的  $p$  阶元素  $h_1, h_2$  属于同一个群，也就证明了这是一个单射。

因此 Sylow  $p$ -子群的个数不多于  $|\mathbb{P}\mathbb{F}_p^2|$ ，也就是说 Sylow  $p$ -子群的个数至多  $p + 1$ ，进一步，它的个数就是  $p + 1$ 。

**Remark.** 我们可以认为上面提到的射影空间是  $\mathbb{F} \cup \{\infty\}$ ，并考虑上面的分式线性变换，我们知道每个元素的稳定子之中恰好有一个 Sylow  $p$ -子群，而且每个 Sylow  $p$ -子群都必然落在一个稳定子之中。前面我们讨论的  $\text{Stab}(\text{span}\{e_1\})$  实际上就是  $\text{Stab}(\infty)$ ，它的唯一一个 Sylow  $p$ -子群是平移变换群。

我们希望说明  $H$  被实现为交换群  $\mathfrak{S}_p \times \mathfrak{S}_p \times \cdots \times \mathfrak{S}_p$  的子群，这等价于证明  $\rho$  是一个单射：这是显然的，如果某个  $h$  在每一个轨道上都是恒等映射，那么它只能是群的单位元素，因此  $\rho$  确实是一个单射。

$H$  作为交换群的子群自然是交换的。

## 17.

类似上题，我们考虑 Sylow  $p$ -子群  $H$  自然地作用于集合  $\{1, 2, 3, \dots, p^2\}$ 。

先证明作用是传递的（等价于说明轨道长度是  $p^2$ ）：若不然，集合由若干个大小为  $p$  的轨道和若干个大小为 1 的轨道组成。如果大小为 1 的轨道数目不为 0，那么至少有  $p$  个，这种情况下  $H$  可以被实现为一个对称群  $\mathfrak{S}_{p(p-1)}$  的子群。对  $p$  的幂次进行计数，我们知道  $H$  不可能是  $\mathfrak{S}_{p(p-1)}$  的一个子群。因此集合由  $p$  个  $p$  阶轨道组成。此时，我们可以构造类似上题的诱导表示：

$$\rho: H \rightarrow \underbrace{\mathfrak{S}_p \times \mathfrak{S}_p \times \cdots \times \mathfrak{S}_p}_{p \uparrow \mathfrak{S}_p}$$

然而，再一次对  $p$  的幂次进行计数，我们知道  $H$  不可能是  $\underbrace{\mathfrak{S}_p \times \mathfrak{S}_p \times \cdots \times \mathfrak{S}_p}_{p \uparrow \mathfrak{S}_p}$  的子群。因此集合的作用是传递的。

由 Jordan 的定理，我们知道至少存在一个  $p^2$ -循环  $g$ ，显然， $\mathfrak{S}_{p^2}$  之中与  $g$  交换的元素只有  $\{1_{\mathfrak{S}_{p^2}}, g, g^2, \dots, g^{p^2-1}\}$ ，因此  $H$  里面包含不和  $g$  交换的元素。

18.

考虑  $H$  在  $\mathfrak{S}_n$  的左诱导表示。作用是传递的  $\Rightarrow$  表示同态的  $\text{Ker}$  不是  $\mathfrak{A}_n$  或  $\mathfrak{S}_n$ ，因此  $\text{Ker}$  是  $\{1_{\mathfrak{S}_n}\}$ ，同时  $H$  被嵌入到了陪集  $1_{\mathfrak{S}_n} \cdot H$  的稳定子群之中。这个稳定子群同构于  $\mathfrak{S}_{n-1}$  的一个子群。再考虑阶数就知道  $H \simeq \mathfrak{S}_{n-1}$ 。

19.

假设阶数为  $p^m (m < k)$  的情形已经得到了证明。同时我们假设  $G$  是非交换群（交换群的情况，由有限生成 Abel 群的分类，我们知道它是  $\mathbb{Z}_p^k$ ，此时命题显然）。

$Z(G)$  非平凡（这是类方程的自然结论）且  $Z(G)$  是  $G$  的真子群：

(1) 如果  $p^l \leq |Z(G)|$ ，那么由归纳假设， $Z(G)$  中有一个阶为  $p^l$  的子群，这个子群是中心的一部分  $\Rightarrow$  它是正规的。

(2) 如果  $p^l > |Z(G)|$ ，假设  $|Z(G)| = p^n$ ，由归纳假设  $G/Z(G)$  一定包含一个阶数为  $p^{l-n}$  的正规子群  $N$ ，显然  $N$  对应了一个  $G$  中的正规子群，它的阶是  $p^l$ 。

□