期中复习题

1. n 是正整数，给出 ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ 的所有子群。

2. G 是群并且它只有有限个子群。证明，G 是有限群。

3. G 是群。对任意的 $g \in G$，共轭映射 $\mathrm{Int}(g)$ 的定义如下：

$$\mathrm{Int}(g) : G \to G, \quad h \mapsto \mathrm{Int}(g)(h) = ghg^{-1}.$$

   证明，以上映射给出群同态：

$$G \to \mathbf{Aut}(G), \quad g \mapsto \mathrm{Int}(g).$$

   并且 $\mathrm{Ker}(\mathrm{Int}) = \mathrm{Z}(G)$ 而 $\mathrm{Im}(\mathrm{Int}) \lhd \mathbf{Aut}(G)$ 是正规子群。

4. $\varphi : G \to A$ 是群同态，A 是交换群。证明，G 中任意的包含 $\mathrm{Ker}(\varphi)$ 的子群都是正规子群。

5. （第二同构定理）G 是群，$K < G$，$N \lhd G$。证明，$N \cap K \lhd K$ 并且有自然的群同构：

$$K\big/_{N \cap K} \xrightarrow{\simeq} NK\big/_{N}.$$

6. G 是群，H, K 为其子群。我们定义 $H \cdot K = \{h \cdot k | h \in H, k \in K\}$。证明，$H \cdot K$ 为子群当且仅当 $H \cdot K = K \cdot H$。

7. G 是群，H, K 为其有限子群。证明，

$$|H \cdot K| = \frac{|H||K|}{|H \cap K|}.$$

8. G 是群，H, K 为其子群。证明，$H \cap K < H$ 并且

$$[H : H \cap K] \leqslant [G : K].$$

   假设 $[G : K]$ 有限，进一步证明以上等号成立当且仅当 $G = K \cdot H$。

9. G 是群，H, K 为其有限指标的子群。证明，

$$[G : H \cap K] \leqslant [G : H][G : K].$$

   并且等号成立当且仅当 $G = K \cdot H$。

10. 当 $n \geqslant 5$ 时，证明，$\mathfrak{S}_n$ 的唯一非平凡正规子群为 $\mathfrak{A}_n$。

11. （对称群指标的另一种定义）定义映射

$$\varepsilon' : \mathfrak{S}_n \to \{\pm 1\}, \quad \sigma \mapsto \varepsilon'(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

   证明，ε' 是群同态并且与之前定义的符号映射 ε 一致。

12. （交换性的一个有用判据）G 是群。证明，G 是交换群等价于 $G\big/_{\mathrm{Z}(G)}$ 是循环群。

13. 群 G 传递地作用在集合 X 上，其中，$|X| \geqslant 2$。证明，该作用是双传递的等价于存在 $x \in X$，使得 $\mathrm{Stab}(x)$ 在 $X - \{x\}$ 上的作用是传递的。

14. （C.Jordan 的定理）有限群 G 传递地作用在有限集 X 上。证明，存在 $g \in G$，使得对任意的 $x \in X$，$g \cdot x \neq x$。

15. （Ore 的定理）G 是有限群，p 是 $|G|$ 的最小素因子，$H < G$ 是子群。如果其指标 $[G : H] = p$，证明，H 是正规子群。

16. p 是素数，计算 $\mathbf{GL}(2; \mathbb{F}_p)$ 的 Sylow p-子群的个数。

17. p 是奇素数，$p \leqslant n < p^2$。证明，$\mathfrak{S}_n$ 的 Sylow p-子群是交换群。

18. p 是奇素数，$n = p^2$。证明，$\mathfrak{S}_n$ 的 Sylow p-子群不交换。

19. $n \geqslant 2$，子群 $H < \mathfrak{S}_n$ 的指标为 n。证明，$H \simeq \mathfrak{S}_{n-1}$。

20. G 是 p-群，$|G| = p^k$。证明，对任意的 $l \leqslant k$，存在正规子群 $H \lhd G$，使得 $|H| = p^l$。（提示：利用 $\mathrm{Z}(G) \neq 1$ 以及 $G \to {}^{G}\!/\!_{\mathrm{Z}(G)}$ 进行归纳）

1. n 是正整数，给出 $\mathbb{Z}/n\mathbb{Z}$ 的所有子群。

解：

$\mathbb{Z}/n\mathbb{Z}$ 为循环群，故其子群也都为循环群

设 M 为 $\mathbb{Z}/n\mathbb{Z}$ 的子群，

由 Lagrange 定理，$|M| \mid n$

取 M 中最小元素 m，考虑 $\langle m \rangle$

$\forall l \in M$，对 m 作带余除法，有 $l = km + r$，　$0 \le r < m$

由 m 定义知 $r = 0 \Rightarrow l = km$

$M = \langle m \rangle$，从而 M 也为循环群

故 $\mathbb{Z}/n\mathbb{Z}$ 的所有子群为 $\{0\}$ 和 $\langle m \rangle$，其中 m 是正整数，且 $m \mid n$.

2. G 是群并且它只有有限个子群。证明，G 是有限群。

证：考虑其逆否命题：若 G 为无限群，则 G 有无穷多个子群

若 G 是一个无限群

取 G 中非单位元元素 a，考虑 a 的阶，若 a 的阶为无穷，

则 $\langle a \rangle \simeq \mathbb{Z}$，有无限个子群；

如不然，即 G 中元素都为有限阶的，那么进行如下操作

取 $g_1 \in G \setminus \{1\}$，得子群 $\langle g_1 \rangle$

再取 $g_2 \in G \setminus \langle g_1 \rangle$，得子群 $\langle g_2 \rangle$

⋮

取 $g_n \in \underbrace{G}_{\text{无限}} \setminus \underbrace{(\langle g_1 \rangle \cup \langle g_2 \rangle \cup \cdots \cup \langle g_{n-1} \rangle)}_{\text{有限}}$，得子群 $\langle g_n \rangle$.

如此进行，则可得无限个子群. #

3. G 是群。对任意的 $g \in G$，共轭映射 $\mathrm{Int}(g)$ 的定义如下：

$$\mathrm{Int}(g): G \to G, \quad h \mapsto \mathrm{Int}(g)(h) = ghg^{-1}.$$

证明，以上映射给出群同态：

$$G \to \mathbf{Aut}(G), \quad g \mapsto \mathrm{Int}(g).$$

并且 $\mathrm{Ker}(\mathrm{Int}) = \mathrm{Z}(G)$ 而 $\mathrm{Im}(\mathrm{Int}) \lhd \mathbf{Aut}(G)$ 是正规子群。

证：先验证 $Int(g) \in Aut(G)$

$$Int(g)(h_1 h_2) = g(h_1 h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = Int(g)(h_1) \cdot Int(g)(h_2)$$

$$Int(g)(1_G) = g \cdot 1_G \cdot g^{-1} = g \cdot g^{-1} = 1_G$$

故 $Int(g)$ 是群同态，显然其为双射，故其为群同构.

而记 映射 $\begin{aligned} G &\longrightarrow Aut(G) \\ g &\longmapsto Int(g) \end{aligned}$ 为 φ.　　其实就是 Int

$\forall h \in G$　$\varphi(g_1 g_2)(h) = Int(g_1 g_2)(h) = g_1 g_2 h (g_1 g_2)^{-1} = g_1 (g_2 h g_2^{-1}) g_1^{-1} = g_1 (Int(g_2)(h)) g_1^{-1}$

$$= Int(g_1)(Int(g_2)(h)) = Int(g_1) \circ Int(g_2)(h) = \varphi(g_1) \cdot \varphi(g_2)(h)$$

故 $\varphi(g_1 g_2) = \varphi(g_1) \cdot \varphi(g_2)$

而 $\varphi(1_G)(h) = Int(1_G)(h) = 1_G h \cdot (1_G)^{-1} = h$.

$\Rightarrow \varphi(1_G) = id_G$

故 φ 为群同态.

而 $g \in Ker(Int) \iff Int(g) = id_G \iff ghg^{-1} = h, \forall h \in G$

$\iff gh = hg, \forall h \in G \iff g \in Z(G)$

从而 $Ker(Int) = Z(G)$.

而 $\forall Int(g) \in Im(Int)$，$\psi \in Aut(G)$，

有 $\psi \circ Int(g) \circ \psi^{-1}(h) = \psi \circ (g \psi^{-1}(h) g^{-1}) = \psi(g) \cdot h \cdot \psi(g^{-1})$

$$= \psi(g) \cdot h \cdot \psi^{-1}(g) = Int(\psi^{-1}(g))(h)$$

从而 $\psi \circ Int(g) \circ \psi^{-1} \in Im(Int)$

$Im(Int) \lhd Aut(G)$

4. $\varphi: G \to A$ 是群同态，A 是交换群。证明，G 中任意的包含 $\mathrm{Ker}(\varphi)$ 的子群都是正规子群。

证：设 $\mathrm{Ker}(\varphi) < H < G$，

$\forall g \in G,\ h \in H$，

有 $\varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1})\varphi(h^{-1})$

$$= \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1}$$

$$\overset{A交换}{=\!=} \varphi(g)\varphi(g)^{-1}\varphi(h)\varphi(h)^{-1}$$

$$= 1_A \cdot 1_A = 1_A$$

$\Rightarrow ghg^{-1}h^{-1} \in \mathrm{Ker}(\varphi)$

$ghg^{-1} \in h\,\mathrm{Ker}(\varphi) \subset H$

故 $H \lhd G$.

5.（第二同构定理）G 是群，$K < G$，$N \lhd G$。证明，$N \cap K \lhd K$ 并且有自然的群同构：

$$K/_{N\cap K} \xrightarrow{\simeq} NK/_{N}.$$

证：$\forall k \in K,\ h \in N \cap K$，显然 $khk^{-1} \in K$

又由 $N \lhd G$，有 $khk^{-1} \in N \Rightarrow khk^{-1} \in N \cap K$

从而 $N \cap K \lhd K$

从而有自然的群同态：

$$\begin{aligned} \varphi:\ K &\longrightarrow G/_N \\ k &\longmapsto kN \end{aligned}$$

$\mathrm{Ker}(\varphi) = \{k \in K \mid kN = N\} = \{k \in K \mid k \in N\} = N \cap K$

$\mathrm{Im}(\varphi) = \{kN \mid k \in K\} = \overset{N正规,\ \exists k' \in K,\ s.t.\ nk' = kn}{\{nk'n^{-1}N \mid k' \in K,\ n \in N\}}$

$= \{nk'N \mid k' \in K, n \in N\} = NK/_N$

由第一同构定理，即有 $K/_{N\cap K} \xrightarrow{\simeq} NK/_N$

6. G 是群，H, K 为其子群。我们定义 $H \cdot K = \{h \cdot k | h \in H, k \in K\}$。证明，$H \cdot K$ 为子群当且仅当 $H \cdot K = K \cdot H$。

证：充分性：若 $H \cdot K = K \cdot H$

则 $\forall\ h_1k_1, h_2k_2 \in H \cdot K$,

$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$

$\exists\ h_3, k_3$ s.t. $(k_1k_2^{-1})h_2^{-1} = h_3k_3$

$\Rightarrow (h_1k_1)(h_2k_2)^{-1} = h_1h_3k_3 \in HK$

$\Rightarrow H \cdot K$ 为子群

必要性：$H \cdot K$ 为子群

$\forall\ h^{-1}k^{-1} \in H \cdot K$, $(h^{-1}k^{-1})^{-1} \in H \cdot K \Leftrightarrow k\,h \in H \cdot K \Rightarrow K \cdot H \subset H \cdot K$

$\forall\ k^{-1}h^{-1} \in K \cdot H$, $(k^{-1}h^{-1})^{-1} = h\,k \in K \cdot H$. $\Rightarrow H \cdot K \subset K \cdot H$

7. G 是群，H, K 为其有限子群。证明，

$$|H \cdot K| = \frac{|H||K|}{|H \cap K|}.$$

证：考虑自然映射 φ: $H \times K \longrightarrow H \cdot K$

$(h, k) \longmapsto hk$

显然这是满射，

定义"$\sim$"　$(h_1, k_1) \sim (h_2, k_2) \Leftrightarrow \varphi(h_1, k_1) = \varphi(h_2, k_2)$

即 $h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$，设为 a.

于是 $h_1 = h_2a$　$k_1 = a^{-1}k_2$

于是可知一个等价类中有 $|H \cap K|$ 个元素，而共有 $|H \cdot K|$ 个等价类，

而 $H \times K$ 中共有 $|H| \cdot |K|$ 个元素.

于是 $|H| \cdot |K| = |H \cdot K| \cdot |H \cap K|$

$$\Rightarrow |H \cdot K| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

8. G 是群，H,K 为其子群。证明，$H\cap K < H$ 并且

显然

$$[H:H\cap K]\leqslant [G:K].$$

假设 $[G:K]$ 有限，进一步证明以上等号成立当且仅当 $G=K\cdot H$。

证：定义映射 f:

$$\{h(H\cap K)\mid h\in H\}\longrightarrow \{gK\mid g\in G\}$$

$$h(H\cap K)\longmapsto hK$$

若 $h(H\cap K)=h'(H\cap K) \Rightarrow h^{-1}h'\in H\cap K$

$\Rightarrow h^{-1}h'K=K$ 映射良定义

$\Rightarrow hK=h'K$

若 $h_1K=h_2K$，那么 $h_1^{-1}h_2\in K$ 从而 $h_1^{-1}h_2\in H\cap K \Rightarrow h_1(H\cap K)=h_2(H\cap K)$

这是一个单射，于是 $[H:H\cap K]\leq[G:K]$

若 $[G:K]$ 有限，

充分性：$G=K\cdot H \overset{由6}{\Longrightarrow}$ f 为满射，从而为双射

等号成立.

必要性：等号成立时，f 为双射

$\Rightarrow$ G 中 K 陪集均可表示为 hK $\Rightarrow G=H\cdot K \underset{由6}{=} K\cdot H$

9. G 是群，H,K 为其有限指标的子群。证明，

$$[G:H\cap K]\leqslant [G:H][G:K].$$

并且等号成立当且仅当 $G=K\cdot H$。

证：由8，只需验证 $[G:H\cap K]=[G:H][H:H\cap K]$

设 $H=\bigcup_{i=1}^{m} h_i(H\cap K)$ $\quad G=\bigcup_{j=1}^{n} g_jH$

于是 $G=\bigcup_{j=1}^{n}\bigcup_{i=1}^{m} g_jh_i(H\cap K)$ $\quad$ 从而 $[G:H\cap K]=mn=[G:H][H:H\cap K]$

进而原命题成立.

10. 当 $n \geqslant 5$ 时，证明，$\mathfrak{S}_n$ 的唯一非平凡正规子群为 $\mathfrak{A}_n$。

证：设 H 为 G_n 的非平凡正规子群，即 $H \lhd G_n$ 且 $H \neq \{1\}$，$H \neq G_n$

于是考虑 $H \cap A_n$，由于 $H \lhd G_n$，$A_n \lhd G_n$ 于是 $H \cap A_n \lhd A_n$

而 A_n $(n \geq 5)$ 是单群，故 $H \cap A_n = \{1\}$ 或 $H \cap A_n = \{A_n\}$

若 $H \cap A_n = \{1\}$，$H \neq \{1\}$ 则 H 含奇置换 σ，但 $\sigma^2 \in A_n$ 矛盾。

若 $H \cap A_n = A_n \Rightarrow A_n \subset H$ 故 $|H| \geq |A_n| \Rightarrow |G_n : H| \leq 2$

故 $|G_n : H| = 2$，从而 $H = A_n$。

#

11.（对称群指标的另一种定义）定义映射

$$\varepsilon' : \mathfrak{S}_n \to \{\pm 1\}, \quad \sigma \mapsto \varepsilon'(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

证明，ε' 是群同态并且与之前定义的符号映射 ε 一致。

证：ε' 是群同态：

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

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

由于 τ 是 $\{1, 2, \cdots, n\}$ 的一个重排，于是 $\tau(i), \tau(j)$ 也遍历 $1 \leq \tau(i) < \tau(j) \leq n$

可记 $k = \tau(i)$，$l = \tau(j)$，于是

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

于是 $\varepsilon'(\sigma\tau) = \varepsilon'(\sigma)\varepsilon'(\tau)$。

显然 $\varepsilon'(1) = 1$，于是 ε' 是群同态

由于对换生成整个置换群，只需证明 $\forall \sigma$ 对换，$\varepsilon'(\sigma) = \varepsilon(\sigma) = -1$

设 $\sigma = (k, l)$ $(k < l)$

$$\text{而 } \varepsilon'(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} = \prod_{\substack{i = k \\ k < j \leq n \\ j \neq l}} \frac{\sigma(i) - \sigma(j)}{i - j} \prod_{\substack{j = l \\ 1 \leq i < l \\ i \neq k}} \frac{\sigma(i) - \sigma(j)}{i - j} \cdot \frac{\sigma(k) - \sigma(l)}{k - l}$$

$$= \prod_{\substack{k < j \leq n \\ j \neq l}} \frac{l - j}{k - j} \cdot \prod_{\substack{1 \leq i < l \\ i \neq k}} \frac{i - k}{i - l} \cdot \frac{l - k}{k - l} = (-1)^{l-k-1} \cdot (-1)^{l-k-1} \cdot (-1) = (-1).$$

#

12. （交换性的一个有用判据）G 是群。证明，G 是交换群等价于 $G/_{Z(G)}$ 是循环群。

证：若 G 是交换群，则 $Z(G)=G \Rightarrow G/Z(G) \simeq \{1\}$.

若 $G/Z(G)$ 是循环群，则 $G/Z(G)=\langle gZ(G)\rangle$

$\forall\, x, y \in G$，有 $x=g^k z_1 \quad y=g^l z_2 \quad z_1, z_2 \in Z(G)$

$xy = g^k z_1 g^l z_2 = g^k \cdot g^l z_1 \cdot z_2$

$= g^l \cdot g^k \cdot z_2 \cdot z_1 = g^l z_2 \cdot g^k z_1 = yx$.

$\Rightarrow$ G 是交换群

13. 群 G 传递地作用在集合 X 上，其中，$|X| \geqslant 2$。证明，该作用是双传递的等价于存在 $x \in X$，使得 $\mathrm{Stab}(x)$ 在 $X-\{x\}$ 上的作用是传递的。

证：若该作用是双传递的，

则 G 在 $X\times X-\Delta$ 上是传递的.

则固定 $x\in X$，任取 $y_1, y_2 \in X-\{x\}$

$\exists\, g\in G$, s.t. $g\cdot(x, y_1) = (g\cdot x, g\cdot y_1) = (x, y_2)$

从而 $g\in Stab(x)$，且 $g(y_1)=y_2$

故 $Stab(x)$ 在 $X-\{x\}$ 上的作用是传递的.

若存在 $x\in X$，使得 $Stab(x)$ 在 $X-\{x\}$ 上的作用是传递的.

即对任意 $y_1, y_2 \in X-\{x\}$，$\exists\, g\in Stab(x)$

s.t. $g(y_1)=y_2$

于是 $\forall\,(x_1, y_1), (x_2, y_2) \in G\times G-\Delta$

取 g_1, s.t. $g_1\cdot x_1 = x$

取 g_2, s.t. $g_2\cdot x = x_2$

再取 $g_3\in Stab(x)$, s.t. $g_3\cdot(g_1\cdot y_1) = g_2^{-1}\cdot y_2$

那么，有 $g_3 g_2 g_1(x_1, y_1) = (x_2, y_2)$

若 (x_i, y_i) 中出现了 x，则不必取 g_1 或 g_2，更简单

于是该作用是双传递的.

14. (C.Jordan 的定理) 有限群 G 传递地作用在有限集 X 上。证明，存在 $g \in G$，使得对任意的 $x \in X$，$g \cdot x \neq x$。

证: 故 $G \curvearrowright X$ 传递，知 $|X| \,\big|\, |G|$

设 $|G| = h|X|$

$\forall x \in X$，其轨道为 X，故其稳定化子 $Stab(x)$ 的阶为 $\frac{|G|}{|X|} = h$

故满足 $g \cdot x = x$ 的 (g, x) 对共有 $h|X| = |G|$

其中，含有形如 $(1_G, x)$ 的对共有 $|X|$ 个，

剩下 $|G|-1$ 的 g 在 (g, x) 对中出现 $(h-1)|X| = |G| - |X|$ 次

故由抽屉原理 $\exists g_0$ 不在任意 (g, x) 对中。 #

15. (Ore 的定理) G 是有限群，p 是 $|G|$ 的最小素因子，$H < G$ 是子群。如果其指标 $[G : H] = p$，证明，H 是正规子群。

证: 考虑自然的群作用
$$G \times G/H \longrightarrow G/H$$
$$(g, g'H) \longrightarrow gg'H$$

从而有自然的群同态 $\varphi: G \to S_{G/H} \simeq S_p$

于是 $G/\ker(\varphi) \simeq Im(\varphi) \subset S_p \Rightarrow |Im(\varphi)| \,\big|\, |S_p| = p!$

若 $|Im(\varphi)| \neq p$，则 $|Im(\varphi)|$ 含有一个小于 p 的素因子 q. $\Rightarrow q \,|\, |G|$,

这与 p 是 $|G|$ 的最小素因子矛盾.

从而 $|Im(\varphi)| = p \Rightarrow |\ker(\varphi)| = \frac{|G|}{|Im(\varphi)|} = \frac{|G|}{p} = |H|$

而 $\forall g \in Ker(\varphi)$，$\varphi(g) = 1_{S_p}$

即 $g \cdot g'H = gg'H = g'H \Rightarrow g'^{-1} g g' \in H$

特别地，取 $g' = 1_G$，有 $g \cdot H = gH = H \Rightarrow g \in H$

从而 $Ker(\varphi) \subset H$ 从而 $H = \ker(\varphi)$，是 G 的正规子群

16. p 是素数，计算 $\mathbf{GL}(2;\mathbb{F}_p)$ 的 Sylow p-子群的个数。

→设为 d

解：$GL(2;\mathbb{F}_p)$ 的元素个数为 $(p^2-1)(p^2-p) = p(p^2-1)(p-1)$

记 $G = GL(2;\mathbb{F}_p)$，N 是 G 的所有 Sylow p-子群构成的集合

考虑 G 在 N 上的共轭作用：

$$G \times N \longrightarrow N$$

$$(g, S) \longmapsto gSg^{-1}$$

已知一个 Sylow p-子群为对角线上均为 1 的上三角矩阵的集合，记为 S

由轨道计数公式，

有 $$\frac{|G|}{|Stab(S)|} = |orb(S)|$$

所有 Sylow p-子群都共轭，则 $|orb(S)|$ 即为 Sylow p-子群的个数

而 $Stab(S) = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$

设 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in N_G(S)$，有

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \quad \forall k = 0, 1, \cdots, p-1.$$

$$\Longleftrightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\Longleftrightarrow \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix} = \begin{bmatrix} a & b+kd \\ c & d \end{bmatrix}$$

得 $c = 0$，$a = kd$.

则 $N_G(S) = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \,\middle|\, a, d \in \mathbb{F}_p^{\times},\ b \in \mathbb{F}_p\right\}$

从而 $|N_G(S)| = (p-1)^2 p$

$$\Longrightarrow |orb(S)| = \frac{|G|}{|N_G(S)|} = \frac{p(p^2-1)(p-1)}{(p-1)^2 p} = p+1.$$

17. p 是奇素数，$p \leqslant n < p^2$。证明，$\mathfrak{S}_n$ 的 Sylow p-子群是交换群。

证：$|S_n| = n!$

由于 $p \leq n < p^2$，不妨设 $kp \leq n < (k+1)p$，$k = 1, \cdots, p-1$

于是 $n!$ 中有 k 个 p 因子.

从而 S_n 的 Sylow p-子群 S 的阶为 p^k.

直接构造

$$H = \langle (1, 2, \cdots, p), (p+1, p+2, \cdots, 2p), \cdots, ((k-1)p+1, \cdots, kp) \rangle$$

可知 $H \simeq (\mathbb{Z}/p\mathbb{Z})^k$，阶为 p^k，是一个 Sylow p-子群.

也是一个交换群

18. p 是奇素数，$n = p^2$。证明，$\mathfrak{S}_n$ 的 Sylow p-子群不交换。

证：$|S_n| = n!$ 共有 $p+1$ 个 p 因子.

Sylow p-子群有 p^{p+1} 个元素.

构造

$$H = \langle (1, 2, \cdots, p), (p+1, p+2, \cdots, 2p), \cdots ((p-1)p+1, (p-1)p+2, \cdots, p^2),$$
$$(1, p+1, \cdots, (p-1)p+1)(2, p+2, \cdots, (p-1)p+2)(p, 2p, \cdots, p^2) \rangle$$

H 内元素个数为 p^{p+1} 个，为 Sylow-p 子群，但它不交换.

19. $n \geqslant 2$，子群 $H < \mathfrak{S}_n$ 的指标为 n。证明，$H \simeq \mathfrak{S}_{n-1}$。

证：通过群作用 $S_n \to S_n/H$

从而诱导自然的同态 $\varphi: S_n \to S_{S_n/H} \simeq S_n$

$\ker\varphi \subset H$，

同时 $\ker\varphi$ 也是 S_n 的正规子群。

由于 $n \neq 4$ 时，S_n 中阶数小于 $(n-1)!$ 的正规子群只有 $\{1\}$

$n=4$ 时，S_n 中阶数小于 $3!$ 的正规子群仅有 $\{1\}$ 与一个4阶子群。

从而由 $|\ker\varphi| \,\big|\, |H|=6 \Rightarrow \ker\varphi = \{1\}$。

于是由 $\ker\varphi=\{1\}$，得知 φ 为单射。

再考虑 $H \curvearrowright S_n/H$

可知 H 中元素都保持 $H \in S_n/H$ 不变，

从而可以将作用限制在 $S_n/H - \{H\}$ 上，获得 H 到 S_{n-1} 的群同态 ψ。

由上知此为单射。又 $|H| = |S_{n-1}| = (n-1)!$ 从而为同构。

即 $H \simeq S_{n-1}$。

20. G 是 p-群，$|G| = p^k$。证明，对任意的 $l \leqslant k$，存在正规子群 $H \lhd G$，使得 $|H| = p^l$。（提示：利用 $\mathrm{Z}(G) \neq 1$ 以及 $G \to G/\mathrm{Z}(G)$ 进行归纳）

证：由于 p-群中心非平凡，于是 $Z(G) \neq \{1\}$ 设 $|Z(G)| = p^m$

1) 若 $m \geq l$，那么取 $Z(G)$ 的 p^l 阶子群即可。

2) 若 $m < l$，考虑 $G/Z(G)$ 其阶为 p^{k-m}，

由归纳假设，其有一个 p^{l-m} 阶的正规子群 N

那么 $NZ(G)$ 即为 G 的 p^l 阶正规子群。