Lec13 Note of Abstract Algebra

Xuxuayame

日期：2023 年 4 月 26 日

我们回忆，对于 $|G| = p^r m,\ (p, m) = 1$，G 的 Sylow p-子群指的是满足 $P \leq G,\ |P| = p^r$ 的子群 P。

记 $N(p)$ 为 Sylow p-子群的数目，那么我们还知道，$N(p) \equiv 1 \mod p$，任意两个 Sylow $p-$ 子群相互共轭，于是 G 可迁地作用在 Sylow p= 子群的集合上，而 $N(p) \mid |G| \Rightarrow N(p) \mid m$。

例 3.1. p, q 素数，$p \neq q$，则 pq 阶群非单，p^2q 阶群非单。

证明. (1) 对于 pq 阶群，不妨设 $p < q$。

由 $N(q) \equiv 1 \mod p,\ N(q) \mid p \Rightarrow N(q) = 1$。于是 G 共轭作用在 Sylow q-子群集合上，且可迁 $\Rightarrow Q \lhd G$，这里 Q 为 Sylow q-子群。

(2) 对于 p^2q 阶群，若 $q < p$，那么 $N(p) \equiv 1 \mod p,\ N(p) \mid q \Rightarrow N(p) = 1$，于是结论成立。

若 $p < q$，则 $N(q) \equiv 1 \mod q,\ N(q) \mid p^2 \Rightarrow N(q) = 1$ 或 p^2。而 p^2 个互不相同的 q 阶子群元素共有 $p^2(q-1)+1$ 个 $\Rightarrow G$ 中 q 阶元共有 $p^2(q-1) \Rightarrow$ 剩下的 p^2 个元素组成唯一的一个 Sylow p-子群。于是结论成立。

$\square$

定理 3.5. 非[1]素数阶循环群的有限单群阶最小为 60，且 60 阶单群同构于 A_5。

证明. 也就是说，$|G| \leq 59 \Rightarrow G$ 为素数阶群或 G 为非单群。于是我们根据以下原则：

- 素数阶群为单群。
- pq, p^2q 阶群非单。
- p^n 阶群非单。

来缩小我们要进一步验证的范围。进一步验证的阶数为 $24, 30, 36, 40, 42, 48, 54, 56$。

当阶数为 $24 = 3 \times 8$ 时，$N(2) = 1$ 或 3，$N(2) = 1$ 时显然成立，若 $N(2) = 3$，设 $S = \mathrm{Syl}_2(G)$，令 G 共轭作用于 S 上，得表示 $\rho\colon G \to S_3$，那么 $\mathrm{Ker}\rho \neq G,\ \mathrm{Ker}\rho \neq \{1\}$，从而 $\mathrm{Ker}\rho$ 为非平凡正规子群。

[1]在这断句。

当阶数为 $30 = 2 \times 3 \times 5$ 时，$N(5) = 1$ 或 6，$N(3) = 1$ 或 10。若 $N(5) = 6$，则 G 中 5 阶元有 $4 \times 6 = 24$ 个，而 $N(3) = 10 \Rightarrow G$ 中含 20 个 3 阶元，矛盾。故必然有 $N(5) = 1$ 或 $N(3) = 1$。

当阶数为 $36 = 4 \times 9$ 时，$N(3) = 1$ 或 4。若 $N(3) = 4$，则 $\rho\colon G \to S_4$, $\mathrm{Ker}\rho \neq G, \{1\}$。

当阶数为 $40 = 5 \times 8$ 时，$N(5) = 1$。

当阶数为 $42 = 2 \times 3 \times 7$ 时，$N(7) = 1$。

当阶数为 $48 = 3 \times 2^4$ 时，$N(2) = 1$ 或 3。若 $N(2) = 3$，则 $\rho\colon G \to S_3$，同理。

当阶数为 $54 = 2 \times 3^3$ 时，$N(3) = 1$。

当阶数为 $56 = 7 \times 2^3$ 时，$N(7) = 1$ 或 8。若 $N(7) = 8$，则有 48 个 7 阶元，剩余 8 个元素组成唯一的 Sylow 2-子群。 □

评论. p^n 阶群非单的缘故在于，根据共轭类方程

$$|G| = |Z(G)| + \sum_{x \in I, |c_x| \geq 2} |c_x|,$$

$|Z(G)|$ 为 p 的倍数，进一步若 G 不交换，那么 $Z(G)$ 必然为非平凡中心，从而为非平凡正规子群。另一方面，如果 G 交换，那么 p-群的存在性指出存在非平凡子群，从而非平凡正规子群。

至于 $\rho\colon G \to S_n$ 的相关问题，$\mathrm{Ker}\rho \neq \{1\}$ 是因为元素个数对不上，ρ 不可能是单同态。另一方面，由于 $|\mathrm{Syl}_p(G)| > 1$，考虑 g 使得一个 Sylow p-子群被共轭到另一个 Sylow p-子群，那么 g 相应的 $\rho_g \neq \mathrm{Id}_{S_n}$，从而 $\mathrm{Ker}\rho \neq G$。

4 自由群与群的表现

4.1 自由群

定义 4.1. 对 $\varnothing \neq S$ 集合，$x, y, z \in S$ 称为**字母**，$x_1 x_2 \cdots x_n$, $x_i \in S$ 称为**单词**或**文字**。

定义**空文字**为空集 $\varnothing$，记为 1。如果文字 w 由 n 个字母组成，那么就说文字 w 的**长度**为 n，记作 $l(w)$。

评论. 更严谨的说法应当是，称 $\{1, \cdots, n\} \to S$ 的映射为长度为 n 的文字。相应的，空文字就是 $\varnothing$ 到 S 的映射，也是空集。

记 $W(S)$ 为 S 上的文字的全体，定义两段文字的运算为：

$$x_1 \cdots x_m \cdot y_1 \cdots y_n = x_1 \cdots x_m y_1 \cdots y_n.$$

那么按定义显然有

$$\begin{aligned}&(x_1\cdots x_m\cdot y_1\cdots y_n)\cdot z_1\cdots z_l\\=&x_1\cdots x_m\cdot(y_1\cdots y_n\cdot z_1\cdots z_l)\\=&x_1\cdots x_m y_1\cdots y_n z_1\cdots z_l.\end{aligned}$$

命题 4.1. $W(S)$ 在上述运算下形成一个含幺半群，称为集合 S 生成的**自由含幺半群**。

进一步可以让 $W(S)$ 诱导出一个群。我们现在找一个和 S 等势的集合，记为 S^{-1}，对应地为每个 $s\in S$ 配对一个 $s^{-1}\in S^{-1}$，并规定 $s\cdot s^{-1}=s^{-1}\cdot s=1$。那么可以验证，$W(S\cup S^{-1})$ 是一个群。

定义 4.2. 称 $w\in W(S\cup S^{-1})$ 为一个**既约文字**，若 w 不含 aa^{-1} 或 $a^{-1}a$，其中 $a\in S$。将 $w=\overline{X}aa^{-1}\overline{Y}$(或 $\overline{X}a^{-1}a\overline{Y}$) 消去 aa^{-1}(或 $a^{-1}a$) 得到一个新文字 $\overline{XY}$ 这一过程称为对 w 的一次**约化**。若既约文字 w' 可由文字 w 经过若干次约化得到，则称 w' 为 w 的一个**既约形式**。

例 4.1. 考虑一段文字 $aa^{-1}acbb^{-1}c^{-1}$。有 $aa^{-1},a^{-1}a,bb^{-1}$ 三处可以约化，依次记为 $1,2,3$。我们现在采用不同的约化顺序，观察最后的既约形式是否一致。

若我们先约化 1 或 2，得到 $acbb^{-1}c^{-1}$，进一步约化 3，得到 acc^{-1}，再得到 a。

若我们先约化 3，得到 $aa^{-1}acc^{-1}$，于是约化 1 或 2 得到 acc^{-1}，再得到 a，或者约化 cc^{-1} 得到 $aa^{-1}a$，从而得到 a。

最后既约形式的一致性并非某种偶然。

引理 4.2. $w\in W(S\cup S^{-1})$ 具有唯一的既约形式。

证明. 对 w 的长度归纳。设命题对长度 $<l(w)$ 的文字成立。我们对 w 可约化处的数量进行讨论。

(1) 若 w 可约化处的数量在两处及以上，我们不妨设 $w=\overline{X}aa^{-1}\overline{Y}bb^{-1}\overline{Z}$，分别约化 aa^{-1} 与 bb^{-1}，得到两个结果 $w_1=\overline{XY}bb^{-1}\overline{Z},w_2=\overline{X}aa^{-1}\overline{YZ}$。
w_1 进一步约化为 $\overline{XYZ}$，而 $l(w_1)<l(w)$，所以 w_1 具有唯一的约化形式，从而 w_1 的约化形式 w' 与 $\overline{XYZ}$ 的约化形式 w'' 相同，$w'=w''$。同理，w_2 约化为 $\overline{XYZ}$，故 $w''=w'''$，w''' 是 w_2 的约化形式。于是 $w'=w'''$。
从而 w 的约化形式唯一，为 w'。

(2) 若 w 可约化的数量仅一处，不妨设 w 具有 $\overline{X}aa^{-1}a\overline{Y}$ 的形式，否则平凡。那么分别约化 aa^{-1} 与 $a^{-1}a$ 得到 $w_1=\overline{X}a\overline{Y},\ w_2=\overline{X}a\overline{Y}$，从而结果显然一致。

(3) 若 w 既约，平凡。

□

于是我们可以定义一个等价关系。在 $W(S\cup S^{-1})$ 上定义 $\sim$ 为：

$$w_1 \sim w_2 :\Leftrightarrow w_1, w_2\text{具有相同的既约形式}.$$

于是考虑 $W(S\cup S^{-1})/\sim$，其完全代表元系即为既约文字。