Lec12 Note of Abstract Algebra

Xuxuayame

日期：2023 年 4 月 21 日

我们补充一个记号，记 G 的全体 Sylow p-子群为 $\mathrm{Syl}_p(G)$。

引理 3.3. $P \in \mathrm{Syl}_p(G)$, $Q \leq G$ 为 p-子群，则 $H = Q \cap N_G(P) = Q \cap P$。

证明. 显然有 $Q \cap P \subset H$，于是我们只需证明 $H \subset Q \cap P$。

由于 $H \subset N_G(P)$，对 $\forall\, h \in H$, $hPh^{-1} = P$。于是我们可以考查 HP，取 $h_1p_1, h_2p_2 \in HP$，那么存在 p_3 使得 $h_2p_3h_2^{-1} = p_1 \Rightarrow h_1p_1h_2p_2 = h_1h_2p_3p_2 \in HP$，于是 HP 在乘法下封闭，进而可以说明 HP 构成群，从而 $HP \leq G$。

那么有 $|HP| = \frac{|H|\cdot|P|}{|H\cap P|}$，由于 $|H|, |H\cap P|$ 均为 p-子群，$|H\cap P| \mid |H|$，所以 $|P| \mid |HP|$，HP 为 p-子群，所以 $P = HP \Rightarrow H \leq P$。 $\square$

于是得到后面两条的证明[1]。

证明. 记 $S = \{gPg^{-1} \mid g \in G\}$，考虑 Q 共轭作用到 S 上。那么

$$S = \mathcal{O}_1 \sqcup \cdots \sqcup \mathcal{O}_s.$$

这里取出 $P_i \in \mathcal{O}_i$, $i = 1, \cdots, s$。那么 $|\mathcal{O}_i| \mid |Q| = p^q \Rightarrow |\mathcal{O}_i| = p^k$, $0 \leq k \leq q$。如果 $\exists\, i\ s.t.\ |\mathcal{O}_i| = 1 \Rightarrow \forall\, q \in Q$, $qP_iq^{-1} = P_i \Rightarrow q \in Q \cap N_G(P_i) = Q \cap P_i \Rightarrow Q \leq P_i$，这由引理 3.3 得到。

于是我们欲证明存在长为 1 的轨道。特别地，我们考查 P 共轭作用在 S 上，轨道长度显然也是 p 的幂次，且 $\{P\}$ 是长为 1 的轨道，下面我们证明它是唯一的。

假设 $\{P_i\}$ 也是长为 1 的轨道，那么 $\forall\, p \in P$, $pP_ip^{-1} = P_i \Rightarrow p \in P \cap N_G(P_i) = P \cap P_i \Rightarrow P \leq P_i \Rightarrow P = P_i$，从而唯一。于是 $|S| \equiv 1 \mod p$。

可见当 Q 共轭作用在 S 上时，必然存在长为 1 的轨道，否则 p 整除轨道长度和，即 $|S|$，矛盾。从而 $\exists\, g\ s.t.\ Q \leq gPg^{-1}$。

特别地，当 Q 是 Sylow p-子群时，$Q = gPg^{-1}$ 与 P 共轭，于是任意两个 Sylow p-子群共轭，且 $\mathrm{Syl}_p(G) = S$。从而 $N(p) := |\mathrm{Syl}_p(G)| \equiv 1 \mod p$。以及 $|\mathrm{Syl}_p(G)| = |S| = |c_P| = |G|/|N_G(P)| \mid |G|$。 $\square$

定理 3.4. $p^k \mid |G|$，记 N 为 p^k 阶子群的个数，则 $N \equiv 1 \mod p$。

[1] 上次 note 有处 typo 没有修正，(2) 中的 Q 为 p-子群。

证明. 令 $S=\{A\subset G \mid |A|=p^k\}$，则 $|S|=\binom{p^r m}{p^k}=\frac{mp^r\cdots(mp^r-p^k+1)}{p^k\cdots 1}$。

考查 G 在 S 上的左乘作用，$g\cdot A=\{ga \mid a\in A\}$。$\forall\, X\in S$，那么 $\mathcal{O}_X$ 中含有一个子群 $\Leftrightarrow |\mathcal{O}_X|=mp^{r-k}\Leftrightarrow G_X=\{g\in G\mid gX=X\}$, $|G_X|=p^k$。且此时 $\mathcal{O}_X$ 中仅有一个形成子群。

进而考虑 G_X 在 X 上的左乘作用，那么 X 在 G_X 作用下是一些 G_X-轨道的并，$X=\bigsqcup G_X\cdot x_i$，进而 $|G_X|\mid|X|=p^k\Rightarrow|\mathcal{O}_X|=\frac{|G|}{|G_X|}=mp^{r-s}$, $0\le s\le k$。

于是我们依次设轨道长度为 mp^{r-k+i} 的轨道数为 N_i，特别地 $N_0=N$，那么

$$
\begin{aligned}
&N\cdot mp^{r-k}+N_1p\cdot mp^{r-k}+\cdots+N_kp^k\cdot mp^{r-k}=\binom{mp^r}{p^k}\\
\Rightarrow &N+p(N_1+\cdots+N_kp^{k-1})=\frac{1}{mp^{r-k}}\binom{mp^r}{p^k}\\
\Rightarrow &N\equiv\frac{1}{mp^{r-k}}\binom{mp^r}{p^k}\mod p\\
\Rightarrow &N\equiv 1\mod p.
\end{aligned}
$$

□

评论. 第一个等价是因为，如果 $\mathcal{O}_X$ 含有一个子群，记为 g_0X，那么 $\mathcal{O}_X=\{gX\mid g\in G\}=\{gg_0X\mid g\in G\}$，从而给出了 g_0X 的所有陪集，于是 $|\mathcal{O}_X|=|G|/|g_0X|=mp^{r-k}$。反过来，如果 $|\mathcal{O}_X|=mp^{r-k}$，则 $|G_X|=p^k=|X|$。取 $g\in X$，那么 $g^{-1}X\in\mathcal{O}_X$ 且 $1\in g^{-1}X$。考虑 $G_{g^{-1}X}=\{h\in G\mid h(g^{-1}X)=g^{-1}X\}$，则 $\forall\, h\in G_{g^{-1}X}$, $h\cdot 1=h\in g^{-1}X\Rightarrow G_{g^{-1}X}\subset g^{-1}X$，而 $|G_{g^{-1}X}|=|G_X|=|X|=|g^{-1}X|$，从而 $g^{-1}X=G_{g^{-1}X}$ 构成群。

而子群的唯一性在于，如果 $\mathcal{O}_X$ 中有 G 的两个子群 $X_1,X_2\le G$，那么 $\exists\, g\ s.t.\ gX_1=X_2\Rightarrow gx_1=1\Rightarrow g^{-1}=x_1\in X_1\Rightarrow gX_1=X_1=X_2$。

推论. $P\in\mathrm{Syl}_p(G)$, $N_G(P)\le A\le G\Rightarrow N_G(A)=A$。

证明. 我们熟知 $A\le N_G(A)$，于是下证 $N_G(A)\subset A$。

设 $g\in N_G(A)$，则 $gAg^{-1}=A$，那么 $gPg^{-1}\le gAg^{-1}=A$，从而 $P\in\mathrm{Syl}_p(A)$，那么 $\exists\, a\in A$ 使得

$$
\begin{aligned}
&gPg^{-1}=aPa^{-1}\Rightarrow(a^{-1}g)P(a^{-1}g)^{-1}=P\\
\Rightarrow &a^{-1}g\in N_G(P)\le A\\
\Rightarrow &g\in A\Rightarrow N_G(A)\subset A.
\end{aligned}
$$

□

推论. $M\lhd G$, $P\in\mathrm{Syl}_p(M)\Rightarrow G=M\cdot N_G(p)$

证明. $\forall\, g\in G$, $gPg^{-1}\le gMg^{-1}=M\Rightarrow gPg^{-1}\in\mathrm{Syl}_p(M)\Rightarrow gPg^{-1}=mPm^{-1}$, $\exists\, m\in M\Rightarrow m^{-1}g\in N_G(P)\Rightarrow g\in M\cdot N_G(P)$。 □