抽象代数学-(VIII)

Lagrange定理展示了有限群的子群的阶整除群的阶。它的反面不对，例如 A_4，$|A_4|=12$，$6|12$，但它没有6阶子群。但是，我们有以下定理(Cauchy定理)

定理 设G是有限群，p素数，$p||G|$，则G包含一个p阶子群.

例如：$p=2\,||G|$. 若$|G|>2$ 考虑$\{g,g^{-1}\}$，$g\in G$，$g\neq g^{-1}$

这取掉G中偶数个元素. 剩余偶数个元素满足$g=g^{-1}$

因为$e=e^{-1}$，故存在$g\neq e$，$g=g^{-1}$，则$\{e,g\}\leq G$.

证明：考虑集合$X=\{(g_1,\cdots,g_p)\,|\,g_i\in G,\ g_1\cdots g_p=e\}$

$\#X=(|G|)^{p-1}$，因为$g_1,\cdots,g_{p-1}$可任选，$g_p=(g_1\cdots g_{p-1})^{-1}$.

考虑$\mathbb{Z}_p$在X上的作用：$\bar{j}\in\mathbb{Z}_p$，$(g_1,\cdots,g_p)\in X$

$\bar{j}*(g_1,\cdots,g_p)=(g_{1+j},\cdots,g_{p+j})$ 这里我们等同

$g_{p+k}=g_k$，即下指标是$\mathbb{Z}_p$中元素

例$j=2$ $(g_3,g_4,\cdots,g_p,g_{p+1},g_{p+2})=(g_3,\cdots,g_p,g_1,g_2)$

$g_3\cdots g_p g_1 g_2=e \Rightarrow (g_3\cdots,g_p,g_1,g_2)\in X$

$\forall x\in X$ $|O_x|=[\mathbb{Z}_p:\mathrm{Stab}.x]=\begin{cases}1 & \Leftrightarrow \forall \bar{j}\in\mathbb{Z}_p,\ \bar{j}*x=x.\\ p\end{cases}$

若$|O_x|=1$，$\forall j\in\mathbb{Z}_p$，$j*x=x$ 则x形如$(g,\cdots,g)$
$g^p=e$ 因此

$$\#X=(|G|^{p-1})\equiv\#\{g\in G\mid g^p=e\}\bmod p$$

但是$|G|^{p-1}\equiv 0\bmod p$ 则$\#\{g\in G\mid g^p=e\}\equiv 0\bmod p$

另一方面$e^p=e$，从而存在$g\neq e$，$g^p=e$.

定义 设G一个群 $|G|<\infty$. p是一个素数. G的一个阶数为p^k $(k\geq 1)$的子群，称为G的p-子群. 若$|G|=p^\ell m$ 且$\ell\geq 1$，$p\nmid m$，则G的p^ℓ阶子群称为G的Sylow p-子群.

令$Syl_p(G)=$ G的Sylow p-子群的集合.

$n_p(G)=\#Syl_p(G)=$ Sylow p-子群的个数.

定理(Sylow) 设G有限群，则

(1) 任意$|G|$的素因子p，均存在G的Sylow p-子群，即

$Syl_p(G)\neq\phi$.

(2) 设$G_1,G_2\in Syl_p(G)$ 则存在$g\in G$，$gG_1g^{-1}=G_2$

且$n_p(G)=[G:N_G(G_1)]$.

(3) 任意p-子群均包含于某一个Sylow p-子群.

(4) $n_p(G)\equiv 1\bmod p$.

例 A_4 只有一个4阶子群 $\{(1),(12)(34),(13)(24),(14)(23)\}$

它是唯一的Sylow 2-子群.

有4个Sylow 3-子群: $\{1,(234),(243)\}$

$\{(1),(123),(132)\}$, $\{(1),(124),(142)\}$, $\{(1),(134),(143)\}$

它们互相共轭.

定理的(1),(3)可加强为:

定理 设G有限群, p素数, $p^n \mid |G|$, $p^{n+1} \nmid |G|$, $n\in\mathbb{N}$.

则有 (1) G含有一个 p^i 阶子群 $\forall 1\le i\le n$.

(2) 每个 $H\le G$, $|H|=p^i$ 均是某个 p^{i+1} 阶子群的正规子群, $1\le i\le n-1$.

证明: 若 $i=1$, 则由Cauchy定理证得.

假设定理对 i 成立, $1\le i\le n-1$. 则存在 $H\le G$, $|H|=p^i$

考虑 H 在 G/H 上作用, $\forall h\in H$, $gH\in G/H$ $h*gH=hgH$

它的轨道的并 $G/H=\bigcup O_g$ $|O_g|=[H:\mathrm{Stab}_g]$

$=\begin{cases}1 \Leftrightarrow \mathrm{Stab}_g=H \Leftrightarrow g\in N_G(H)\\ p^k, k\ge 1\end{cases}$

$\Rightarrow |G/H|\equiv\left|\frac{N_G(H)}{H}\right| \bmod p$ 若 $p \mid |G/H|$, 则 $p \mid \left|\frac{N_G(H)}{H}\right|$,

由Cauchy定理, 存在 $K\le \frac{N_G(H)}{H}$ $|K|=p$.

考虑 $\pi: N_G(H)\longrightarrow \frac{N_G(H)}{H}$ 则 $\pi^{-1}(K)\le G$, $H\le\pi^{-1}(K)$

$\frac{\pi^{-1}(K)}{H}\cong K \Rightarrow |\pi^{-1}(K)|=p^{i+1}$

因为 $H \lhd N_G(H)$，$H \lhd \pi^{-1}(K)$.

例 若G是p^r阶群，$r\geq 2$，则G非单群.

下证第二Sylow定理，即主定理(2)的第一部分.

设 $G_1, G_2 \in Syl_p(G)$ 考虑G_2在 G/G_1 上作用，正如前，

$G/G_1 = \bigcup O_g$ $\quad |O_g| = [G_2 : \mathrm{Stab}.g] =$

$\begin{cases} 1 \Leftrightarrow \mathrm{Stab}.g = G_2 \\ p^k,\ k\geq 1 \end{cases}$ $\quad \forall x\in G_2,\ g^{-1}xg\in G_1 \Leftrightarrow g^{-1}G_2g=G_1$

令 $X=\{g\in G \mid g^{-1}G_2g=G_1\}$

$\Rightarrow |G/G_1| \equiv |X| \mod p$ 因为 $p\nmid |G/G_1|$，$|X|\neq 0$

$\exists g\in X$，$g^{-1}G_2g=G_1$

下证第三Sylow定理，即主定理关于$n_p(G)$的刻划

考虑P在$Syl_p(G)$上作用：

证明：设$P\in Syl_p(G)$，

$\forall x\in P$，$Q\in Syl_p(G)$ $\quad xQx^{-1}\in Syl_p(G)$ $\quad P, Q$是$N_G(Q)$的Sylow子群 $\Downarrow$ 在$N_G(Q)$中

若 $xQx^{-1}=Q$ $\forall x\in P$，由第二Sylow定理，P, Q共轭

且 $P, Q\leq N_G(Q)$ $\quad Q\lhd N_G(Q) \Rightarrow P=Q$. 因此

① $n_p = |Syl_p(G)| \equiv 1 \mod p$.

考虑G在$Syl_p(G)$上作用，由第二Sylow定理. $Syl_p(G)$

只有一个轨道 它的阶数 $=[G:\mathrm{Stab}\,Q]=[G:N_G(Q)]$

例1 设G是有限群, $|G|=20$, 由第三Sylow定理. $p=5$

$n_5 \mid 20$, $n_5 \equiv 1 \bmod 5 \Rightarrow n_5=1$, 必须正规子群 $\Rightarrow$ G非单群

例2. 设G有限群, $|G|=30$. $p=5$, $n_5 \mid 30$, $n_5 \equiv 1 \bmod 5$

则 $n_5=1$或6. $n_3 \mid 30$, $n_3 \equiv 1 \bmod 3$ 则 $n_3=1$或10.

若 $n_5=6$, 任两个Sylow 5-子群交为$\{e\}$ $\Rightarrow$ G包含

$4\times 6=24$个5阶元, 此时, 3阶元个数≤ 5 $\Rightarrow n_3=1$.

若 $n_3=10$, 则有 2×10个3阶元 $\Rightarrow n_5=1$.

即G有一个5阶或3阶正规子群 $\Rightarrow$ G非单群.

例3. 设G是一个pq阶群, $p\neq q$ 素数. $p\nmid q-1$, $q\nmid p-1$, 则

G是循环群.

证明: G的Sylow p-子群个数 $n_p \mid pq$ 且 $n_p \equiv 1 \bmod p$.

$\Rightarrow n_p \mid q$ $\quad n_p=1$或q $\quad p \mid n_p-1$ $\quad p\nmid q-1 \Rightarrow n_p=1$.

同理 $n_q=1$ 令 $P=\langle a\rangle$, $Q=\langle b\rangle$ $\quad |P|=p$, $|Q|=q$

$P\cap Q \le P$, $P\cap Q \le Q \Rightarrow P\cap Q=\{e\}$ $\quad aba^{-1}b^{-1}\in P\cap Q$

$aba^{-1}b^{-1}=e \Rightarrow ab=ba$ $\quad o(ab)=pq$. $G=\langle ab\rangle$

作业: Page53 1, 4, 5, 6, 9, 13.