2018.10.4

Date

§2. 西罗定理.

拉格朗日定理：若 $H \leq G$ 为子群 则 $|H| \mid |G|$.

例. 1) A_4 中不存在6阶子群

(证：设 $|H|=6$. $\pi \in A_4$ 为3-循环. 则 $\langle \pi \rangle \cap H \neq \{1\}$

否则 $|\langle \pi \rangle H| = 3 \cdot |H| = 18 > 12$. $\therefore \pi \in H$.

$\therefore H$ 含 A_4 中所有3-循环. $\Rightarrow H = A_4$ 矛盾 □)

2) 非交换单群 G 中不存在 $\frac{|G|}{2}$ 阶子群.

定义. 设 p 为素数.

1) 若 $|G| = p^s$ 其中 $s \geq 0$ 则称 G 为 p-群

2) 设 $|G| = p^n m$ 其中 $\gcd(p, m) = 1$. G 中阶为 p^n 的子群称为 G 的一个西罗 p-子群.

注：由拉格朗日定理 西罗 p-子群是 G 中的极大 p-子群.

例：1) $G = GL_n(\mathbb{Z}/p\mathbb{Z})$ 其中 p 为素数.

$$|G| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{\frac{n(n-1)}{2}} \cdot m.$$

$$U = \left\{ A \in GL_n(\mathbb{Z}/p\mathbb{Z}) \mid A = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}.$$

则 $|U| = p^{n-1} \cdot p^{n-2} \cdots p \cdot 1 = p^{\frac{n(n-1)}{2}}$ $\therefore U$ 为 G 的西罗 p-子群.

2) $|A_4| = 12 = 2^2 \cdot 3$

$V_4 \lhd A_4$ ~~$|V_4| =$~~ V_4 是 A_4 的西罗2-子群且唯一.

A_4 的西罗3-子群：$\langle (123) \rangle$ $\langle (124) \rangle$ $\langle (134) \rangle$ $\langle (234) \rangle$.

Date

引理1：设p为素数，$a \geq b \geq 0$，$m \geq 0$，则 $\binom{p^m a}{p^m b} \equiv \binom{a}{b} \bmod p$.

证：注意到 $\forall 0 < m < p$ 有 $p \mid \binom{p}{m}$.

$\therefore (X+1)^{pa} = (X^p + \binom{p}{1}X^{p-1} + \cdots + 1)^a \equiv (X^p+1)^a \bmod p$

迭代n次有：$(X+1)^{p^n a} \equiv (X^{p^n}+1)^a \bmod p$

比较 $X^{p^n b}$ 系数有 $\binom{p^n a}{p^n b} \equiv \binom{a}{b} \bmod p$.

引理2：设P为G的西罗p-子群，Q为G的p-子群，则 $N_G(P) \cap Q \subseteq P$.

~~证：设 $a \in N_G(P) \cap Q$，令 $H = N_G(P) \cap Q$，则 H 为 G 的 p-群~~

证：由 BA III. P.12 公式：$|G| = (G : N_G(P))(N_G(P) : P)|P|$.

$\therefore \left| \frac{N_G(P)}{P} \right| \mid m$.

设 $a \in N_G(P) \cap Q$，则 $\exists l \mid m$ s.t. $(aP)^l = P$.

又 $\because a \in Q$，$\therefore \exists l'$ s.t. $a^{p^{l'}} = 1 \Rightarrow (aP)^{p^{l'}} = P$.

$\because \gcd(p^{l'}, l) = 1$，i.e. $\exists u, v$ s.t. $up^{l'} + vl = 1$

$\therefore aP = (aP)^{up^{l'}}(aP)^{vl} = P \quad \therefore a \in P$.

定理1（第一西罗定理）~~设 $|G| = p^n m$，其中~~ 西罗p-子群存在.

证：设 $|G| = p^n m$，其中 $\gcd(p, m) = 1$.

令 $\Omega = \{M \subseteq G \mid |M| = p^n\}$（$M$为子集）.

考虑群作用：$G \times \Omega \longrightarrow \Omega$

$(g, M) \longrightarrow \{ga \mid a \in M\}$

设 $\Omega = \bigcup_i \Omega_i$ 为轨道分解，则

Date

$|\Omega| = \sum_i |\Omega_i| = \sum_i (G : St(M_i))$ 其中 $M_i \in \Omega_i$.

$\because St(M_i)M_i = M_i \quad \therefore M_i = \bigcup_j St(M_i)g_{ij}$ 都能分解.

$\therefore |St(M_i)| \mid |M_i| = p^n \quad \therefore \forall i \quad |St(M_i)| = p^{m_i} \quad m_i \le n$

1) 若 $\exists i_0$ s.t $|St(M_{i_0})| = p^n$ 则 $St(M_{i_0})$ 为西罗 p-子群

2) 设 $\forall i \quad |St(M_i)| < p^n$ i.e. $m_i \le n-1$.

则 $(G : St(M_i)) = \left| \frac{G}{St(M_i)} \right| = m p^{n-m_i}$

$\therefore \forall i \quad p \mid (G : St(M_i))$.

$\therefore p \mid |\Omega|$. $\because |\Omega| = \binom{p^n m}{p^n}$ 由引理1 $p \nmid |\Omega|$. 矛

定理2 (第二西罗定理). 设 P 为 G 的西罗 p-子群. Q 为 G 的 p-子群. 则 $\exists g \in G$ s.t $Q \le gPg^{-1}$. 特别地 西罗 p-子群均共轭.

证: 令 $\Omega = G/P$. 考虑群作用: $Q \times \Omega \to \Omega$

$(g, aP) \longrightarrow gaP$

设 $\Omega = \bigcup_i \Omega_i$ 轨道分解. 则 $|\Omega| = \sum_i |\Omega_i| = \sum_i (Q : St(a_iP))$ 其中 $a_iP \in \Omega_i$.

$\therefore |\Omega_i| = p^{k_i} \quad k_i \ge 0 \quad \forall i$.

$\because p \nmid |\Omega| = m \quad \therefore \exists i_0$ s.t $|\Omega_{i_0}| = p^0 = 1$.

此时 $Q a_{i_0} P = a_{i_0} P$ i.e $Q a_{i_0} P a_{i_0}^{-1} = a_{i_0} P a_{i_0}^{-1}$

$\therefore Q \le a_{i_0} P a_{i_0}^{-1}$

当 Q 为西罗 p-子群时有 $Q = a_{i_0} P a_{i_0}^{-1}$.

Date

定理3（第三西罗定理）设 $N_p=|\{G\text{的西罗}p\text{-子群}\}|$，则 $N_p=(G:N_G(P))$，P为西罗p-子群 且 $N_p\equiv 1 \bmod p$.

证：令 $\Omega=\{G\text{的西罗}p\text{-子群}\}$

考虑群作用：$G\times\Omega\longrightarrow\Omega$

$(g,Q)\longrightarrow gQg^{-1}$

则 $N_G(P)=St(P)=\{g\in G\mid gPg^{-1}=P\}$.

由定理2，此类轨作用是可迁的. i.e. $\Omega=G(P)$.

$\therefore N_p=|\Omega|=(G:St(P))=(G:N_G(P))$.

考虑 $P\times\Omega\longrightarrow\Omega$ （此时却为可迁的）.

$(g,Q)\longrightarrow gQg^{-1}$

设 $\Omega=\bigcup_i\Omega_i$ 为轨道分解.

1) 只有一个轨道其长度为1.

设 $|\Omega_{i_0}|=1$. 令 $\Omega_{i_0}=\{Q_{i_0}\}$.

则 $\forall g\in P$ $gQ_{i_0}g^{-1}=Q_{i_0}$ i.e $P\subseteq N_G(Q_{i_0})$

由引理2：$P\subseteq Q_{i_0}$ $\therefore P=Q_{i_0}$.

2) 又 $\because |\Omega_i|=(P:St(Q_i))\mid |P|=p^n$，这里 $P_i\in\Omega_i$.

$\therefore$ 若 $|\Omega_i|>1$ 则 $p\mid|\Omega_i|$

综上：$N_p=|\Omega|=|\Omega_{i_0}|+\sum_{i\neq i_0}|\Omega_i|\equiv 1 \bmod p$.

Date

例: $G=SL_2(\mathbb{Z}/p\mathbb{Z})$ p为素数.

~~Ker~~ $\det: GL_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$

$A \longrightarrow \det(A)$

$|GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$ $\quad |(\mathbb{Z}/p\mathbb{Z})^*| = p-1$

$\therefore |SL_2(\mathbb{Z}/p\mathbb{Z})| = p(p^2-1)$.

西罗p-子群: $P=\left\{\begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix} \middle| \alpha \in \mathbb{Z}/p\mathbb{Z}\right\}$ $\overline{P}=\left\{\begin{pmatrix}1 & 0\\ \alpha & 1\end{pmatrix} \middle| \alpha \in \mathbb{Z}/p\mathbb{Z}\right\}$

$\therefore N_p = 1+lp > 1$.

又: $\begin{pmatrix}\lambda & \beta\\ 0 & \lambda^{-1}\end{pmatrix}\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}\begin{pmatrix}\lambda^{-1} & -\beta\\ 0 & \lambda\end{pmatrix} = \begin{pmatrix}1 & \lambda^2\alpha\\ 0 & 1\end{pmatrix}$

$\therefore H=\left\{\begin{pmatrix}\lambda & \beta\\ 0 & \lambda^{-1}\end{pmatrix} \middle| \begin{matrix}\lambda \in (\mathbb{Z}/p\mathbb{Z})^*\\ \beta \in \mathbb{Z}/p\mathbb{Z}\end{matrix}\right\} \subseteq N_G(P) \Rightarrow N_G(P) \geq p(p-1)$

$\therefore N_p = p+1$

结论: $SL_2(\mathbb{Z}/p\mathbb{Z})$中的西罗$p$-子群不是正规子群.

注: $PSL_2(\mathbb{Z}/p\mathbb{Z}) = SL_2(\mathbb{Z}/p\mathbb{Z})/\{\pm 1\}$ 是单群.

~~定理4~~: ($\mathbb{P}(\mathbb{Z}/p\mathbb{Z}) = \{0,1,\cdots,p-1\}\cup\{\infty\}$上的变换群

$A \in PSL_2(\mathbb{Z}/p\mathbb{Z})$ $\quad x \longrightarrow \dfrac{a_1x+a_2}{a_3x+a_4}$

$\begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix}$)

~~定理4~~: i) G中的西罗p-子群是正规的 $\Leftrightarrow N_p=1$

ii) 设 $|G| = p_1^{n_1}\cdots p_k^{n_k}$. 则 $\forall 1\leq i\leq k$ G的西罗p_i-子群是正规的 $\Leftrightarrow G \cong P_1\times P_2\times\cdots\times P_k$ 这里P_i是p_i-群

Date

定理4: i) G 关于素数 p 的 Sylow p-子群在 G 中正规 $\Leftrightarrow n_p=1$.

ii) 设 $|G|=p_1^{n_1}\cdots p_k^{n_k}$ 且 $P_1,\cdots P_k$ 为 G 的 Sylow p_i-子群

则 $\forall 1\le i\le k$, P_i 在 G 中正规 $\Leftrightarrow G\cong P_1\times P_2\times\cdots\times P_k$.

证: i) 设 P 为 G 的 Sylow p-子群. 由第二 Sylow 定理.

~~$P\lhd G\Leftrightarrow \forall g\in G\ gPg^{-1}=P\Leftrightarrow n_p=1$~~

若 Q 为 G 的 Sylow p-子群 则 $\exists g\in G$ s.t. $Q=gPg^{-1}$, $P\lhd G$

$\Rightarrow Q=P\Rightarrow n_p=1$.

$n_p=1$, $\forall g\in G$, gPg^{-1} 为 G 的 Sylow p-子群 $\Rightarrow \forall g\in G\ gPg^{-1}=P$

$\Rightarrow P\lhd G$.

ii) ($\Rightarrow$)

① $\forall\ 1\le i\ne j\le k$ $P_i\cap P_j=\{1\}$.

$\forall a\in P_i\cap P_j\Rightarrow a^{p_i^{n_i}}=1=a^{p_j^{n_j}}$, $\gcd(p_i^{n_i},p_j^{n_j})=1$

$\Leftarrow \exists u,v$ s.t. $up_i^{n_i}+vp_j^{n_j}=1$

$\Rightarrow 1=a^{up_i^{n_i}+vp_j^{n_j}}=a$

② $\forall 1\le i\ne j\le k$ $\forall a\in P_i$, $b\in P_j$ $ab=ba$

$aba^{-1}b^{-1}\in P_i\cap P_j=\{1\}\Rightarrow ab=ba$.

③ 若 $a_1a_2\cdots a_k=1$ 其中 $a_i\in P_i$ 则 $\forall i$, $a_i=1$.

$\forall$ 令 $m_i=\prod_{j\ne i}p_j^{n_j}$.

$a_1a_2\cdots a_k=1\Rightarrow a_i^{-1}=a_1a_2\cdots\hat{a_i}\cdots a_k$

$\Rightarrow (a_i^{-1})^{m_i}=(a_1a_2\cdots\hat{a_i}\cdots a_k)^{m_i}=1$

(由①, $a_{j_1}a_{j_2}=a_{j_2}a_{j_1}$)

又 $(a_i^{-1})^{p_i^{n_i}}=1$

$\therefore a_i^{-1}=1\Rightarrow a_i=1$.

Date

⑧令 $H = P_1 P_2 \cdots P_k$ 则 $|H| = p_1^{n_1} \cdots p_k^{n_k} \Rightarrow H = G$.

定义: $\varphi: P_1 \times P_2 \times \cdots \times P_k \longrightarrow G$

$(a_1, a_2, \cdots a_k) \longrightarrow a_1 a_2 \cdots a_k$

由① $a_{i_1} a_{i_2} = a_{i_2} a_{i_1} \Rightarrow \varphi$ 是群同态

由④ φ 为满同态. 而由③ φ 为单射 $\therefore \varphi$ 为同构.

($\Leftarrow$) 设 $\varphi: P_1 \times P_2 \times \cdots \times P_k \longrightarrow G$ 为群同构.

~~则 $\varphi(P_1 \times \cdots \times P_i \times \cdots \times \{1\})$~~ 令 $H_i = \varphi(\{1\} \times \cdots \times P_i \times \cdots \times \{1\})$

则 H_i 为 G 的正规子群 且 H_i 为 G 的西罗 p_i-子群.

由① $N_{p_i} = 1$ $\therefore H_i = P_i$ $\therefore P_i \trianglelefteq G$.