U1: (Sylow Thm. existence). $|G|=p^r m$, $\gcd(p,m)=1$, $p\in$ Prime; $\exists |H|=p^r$ $H\in Syl_p(G)$

induct on order: 比 $|G|$ 小皆可用

1. if $p\nmid |Z(G)|$

$|G|=|C(a_1)|+|C(a_2)|+\cdots|C(a_n)|+|Z(G)|$

$\exists\ p\nmid |C(a_i)|$

$|G|=|C(a_i)|\times|C_G(a_i)|$ $\therefore |C_G(a_i)|=p^r\overline{m}$ $C_G(a_i)\in Sylow_p(G)$ 这里可能有m因子，但由于 induct 可以再在 $C_G(a)$ 中找

2. if $p\mid |Z(G)|$

2.1 if $|Z(G)|=|G|$, refer to finite Abel group $\exists H=\{x\in G: x^{p^r}=e\}\in Syl_p(G)$

2.2 if $|Z(G)|<|G|$, $\exists N\in Sylow_p(Z(G))$ by induction

$N\leq Z(G)$ $\therefore N\lhd G$ and $|G/N|<|G|$; $|N|=p^{r_1}$

$\exists\ P/N\in Sylow_p(G/N)$

Let $\bar{P}=\{x\in G: xN\in P/N\}$, $|N|=p^{r_1}$, $|G/N|=p^{r-r_1}m$, $|P/N|=p^{r-r_1}$

$|\bar{P}|=|P/N|\times|N|=p^r$

即 $\bar{P}\in Sylow_p(G)$, 证毕

共轭 group 与 group $\begin{cases} X=g^{-1}Yg & |X|=|Y| \\ 每个X的元素与Y中元素共轭 \end{cases}$

(Sylow Thm. conjugation): $|G|=p^r m$, $P\in Sylow_p(G)$, 若 $|H|\mid p^n$ some n, H conjugate to subgroup of P. $\Rightarrow\begin{cases}\text{Sylow-}p\text{ subgroup conjugate}\\ P\lhd G,\ \text{Sylow-}p\text{ subgroup unique}\end{cases}$

1. G act on $[G:P]=\{xP: x\in G\}$

$g: [G:P]\to[G:P]$, $\check{g}$ 用右乘方便一点 $[G:P]=\{Px: x\in G\}$ 就行

$xP\to g^{-1}xP$ 通过 $x^{-1}G(xP)x$ 共轭

$\forall x$, the stablizer $G(xP)$ conjugate to $G(P)=P$ since:

$\begin{cases} g\in G(xP)\quad g^{-1}xP=xP, \text{ then } (x^{-1}g^{-1}x)P=x^{-1}(xP)=P;\ x^{-1}g^{-1}x,\ x^{-1}gx\in \overset{\text{group}}{G(P)} \\ g\in G(P),\ g^{-1}P=P, \text{ then } (xg^{-1}x^{-1})xP=xg^{-1}P=xP;\ xg^{-1}x^{-1},\ xgx^{-1}\in G(xP)\end{cases}$

$G(P)=P$ obv $x^{-1}G(xP)x=G(P)$ ✓

2. H act on $[G:P]=\{xP: x\in G\}$, $|H|=p^n$ some $n\leq r$

$h: [G:P]\to[G:P]$ $\check{h}$

$xP\to h^{-1}xP$

$\exists$ some x_1P s.t. H fix x_1P, $H(x_1P)=H$ $(x_1P)^H=x_1P$ since:

if $(x_1P)^H \cap (x_2P)^H = h_1^{-1}x_1P = h_2^{-1}x_2P$

then: $x_1P = h_1h_2^{-1}x_2P$, thus come to $(x_1P)^H = (x_2P)^H$ 形成一个等价类

$\therefore [G:P] = (x_1P)^H \cup (x_2P)^H \cup \cdots (x_nP)^H$; $m = |[G:P]| = |(x_1P)^H| + \cdots |(x_nP)^H|$

$|H| = |(x_iP)^H| \times |H_{(x_iP)}|$

$|(x_iP)^H| = 1$ or $p^{()}$, since $\gcd(m,p)=1$

$\therefore \exists$ say: $(x_iP)^H = x_iP$; x_iP 是 H 的不动点

1+2: $G_{(xP)} \sim G_{(P)} = P$, 取 $x = x_i$

$H_{(xP)}$ is subgroup of $G_{(xP)}$ since $H \le G$.

$\therefore H = H_{(xP)} \sim$ subgroup of P 证毕

* $G_a \sim G_{(ga)}$ $\forall a \in \Omega, g \in G$ 有什么用? $\Rightarrow$ Sylow Thm 重要

(Sylow Thm. $|\mathrm{Sylow}_p(G)| = n_p$, $|G| = p^r m$, $n_p \mid m$; $n_p \equiv 1 \pmod p$

$|G| = p^r q^s$ 时

n_p 不是 $n_p \mid q$ 是 $n_p \mid q^s$ 期中错了!

1. consider P act on $\mathrm{Sylow}_p(G)$

$\tilde{p}: \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G)$

$X \to p^{-1}Xp$

$\therefore |\mathrm{Sylow}_p(G)| = |X_1^P| + |X_2^P| + \cdots |X_n^P|$

$|P| = |X_i^P| \times |P_{X_i}|$, $|X_i^P| = 1$ or $|X_i^P| = p^{()}$

仅当 $X_i = P$, $|X_i^P| = 1$, P fix X_i since:

$P = P_{X_i} \le N_G(X_i)$; $X_i \le N_G(X_i)$ obv

$\therefore P, X_i \in \mathrm{Sylow}_p(N_G(X_i))$

$X_i \trianglelefteq N_G(X_i)$ obv, by Thm $P = y^{-1}X_iy = X_i$ $\Rightarrow |\mathrm{Sylow}(G)| = 1 + p^{()} + p^{()} + \cdots p^{()}$

$\therefore n_p \equiv 1 \pmod p$

2. consider G act on $\mathrm{Sylow}_p(G)$

$\tilde{g}: P \to g^{-1}Pg$, g

$|G| = |P^G| \times |G_P| = |\mathrm{Sylow}(G)| \times |N_G(P)|$ (G_P)

为什么 $P^G = \mathrm{Sylow}_p(G)$

已知 Sylp 之间共轭, 但共轭后定 Sylp?

$\therefore |\mathrm{Sylow}(G)| = \frac{|G|}{|N_G(P)|}$

$\frac{|G|}{|N_G(P)|} \times \frac{|N_G(P)|}{|P|} = m$, $\frac{|N_G(P)|}{|P|}$ is integer since $P \le N_G(P)$

$\therefore |\mathrm{Sylow}(G)| \mid m$

是 $g^{-1}Pg$ 形式吗

HW5.5 (1) $|G|=pq$, G is not simple：Normal group只有e和G

$n_p | q$, $n_p \equiv 1 \pmod p$

1. $n_p=1$ done if $n_p=1$ 为什么可以证normal，Sylow Thm3 证明 $g^{-1}Pg\in Syl_p$ 为什么?

2. $n_p=q$. $n_q | p$. $n_q \equiv 1 \pmod q$ CAA的Sylow 2 P392

   2.1 $n_q=1$ done

   2.2 $n_q=p$. $q=kp+1$. $p=nq+1$

   count element in G: $q(p-1)+p(q-1)+1 > pq$ 为什么

p阶Sylow群之间为什么没有交集(e除外)

不同p阶和q阶之间也不交吗?

Sylow有p阶 → p为质数

∴G_{p_1}和G_{p_2}没有e外的交

CAA P395. $|G|=40=2^3\times 5$

$n_5 | 2$, $n_5 \equiv 1 \pmod 5$ ∴ $n_5=1$

仅有一个$Sylow_5(G)$元素 ∴ 它is normal

if $n_8=1$, 它is normal

if $n_8=5$, none is normal, 且 P_1, P_2, P_3, P_4, P_5 可以用 xP_1x^{-1}表示

记5阶群G_5. 8阶群G_8. $G=G_5G_8$

if $n_8=1$, $G_8 \triangleleft G$. $G_5 \triangleleft G$ then $G=G_8\times G_5$

p阶sylow群之间没交集(e除外)

但p^n阶和p^n阶会有的!

$|A|=p^n, |C|=q^m$ $x\in A\cap C$

$o(x) | |A|$ $o(x) | |C|$

但$|A|$$|C|$ 阶互质 ∴ $o(x)=1$

$x=e$

⇒ 群order互质 交为e

$|G|=30=2\times 3\times 5$

$n_5 | 6$. $n_5 \equiv 1 \pmod 5$, $n_5=1$ or 6

$n_3 | 10$. $n_3 \equiv 1 \pmod 3$, $n_3=1$ or 10

但其中$n_5=6$和$n_3=10$不同时取，不然总个数超出30

∴ 5阶sylow群和3阶Sylow群至少有一个normal to G

∴ $|G_3G_5|=15$, then $G_3G_5 \triangleleft G$, G_3G_5 cylic

因为至少有一个$G_i \triangleleft G$ ∴可构成subgroup. $G_3G_5 \triangleleft G_5$是因为 $[G:H]=2 \Rightarrow H \triangleleft G$

$\Leftarrow p\nmid q-1,\ q\nmid p-1$

cyclic: CAA P396: $|G|=p\cdot q$, $p,q\in$ Prime, $p<q$ 且 $p\nmid q-1$; G is cyclic

let $K\in Sylow_q(G)$, $H\in Sylow_p(G)$

∵ $n_p \equiv 1 \pmod p$, $n_p | q$ $n_p=pz+1 | q$, $z\in \mathbb{Z}^+$

∴ $pz+1=q$ (舍) or $pz+1=1$, then $z=0$ $n_p=1$

同样的 $n_q=qz'+1 | p$, $z'\in \mathbb{Z}^+$

∴ $qz'+1=1$ or $qz'+1=p$ ($p-1<q$ ∴ $z'=0$), $n_q=1$

∴ $G_p \triangleleft G$. $G_q \triangleleft G \xRightarrow{\cap = e} G_p\times G_q = G \cong \mathbb{Z}_p\times \mathbb{Z}_q = \mathbb{Z}_{pq}$

CAAP39 Sylow 2: $H \le G$, $|H| = p^r$, then $H \le$ some Sylow p subgroup of G

已证: Sylow p subgroups conjugate; $P \in Syl_p$, $Q \in Syl_p$, $P \sim Q$

$\Rightarrow P \in Syl_p$, $\forall g \in G$, $g^{-1}Pg = Q$ some $Q \in Syl_p$

$P \lhd G$, 只有唯一一个 Syl_p 子群 P $\overset{\Leftarrow}{\Rightarrow}$ since $g^{-1}Pg = P$

$\Rightarrow$ 只有一个 Syl_p 子群, $\therefore \forall y \in G$ $y^{-1}Py = P$ $\therefore P \lhd G$

HW5.2. $|G| = p^2 q$, G is not simple

$n_p \equiv 1 \pmod q$, $n_p | q$ $n_p = 1$ (done) or $n_p = q$

$n_p = q$: $n_q | p^2$, $n_q \equiv 1 \pmod q$ $\therefore n_q = 1$ (done) or p, p^2

1. $n_q = p^2$

从个数判断 $\Rightarrow \begin{cases} p^2(q-1) + q(p^2-1) < p^2 q & \text{可能满足} \\ \text{但: } p^2 q - p^2(q-1) = p^2, \text{这 } p^2 \text{ 个元素无法形成 } q \text{ 个 Sylow p 子群} \end{cases}$

since $p^2 > q(p^2-1) + 1$ implies $p < 1$ (舍)

2. $n_q = p$, $p \equiv 1 \pmod q$

$q \equiv 1 \pmod p$ 两式矛盾

例. HW3.8 A_4 不会有 order $= 6$ 的子群

设 $|H| = 6$. $H \le A_4$ $|[A_4 : H]| = 2$ $\therefore H \lhd A_4$ A_4/H well-defined

1. 设 H contains $\forall$ 3-cycles

$(123)(132), (124)(142), \cdots$ 不含 1.2.3.4 的 3-cycle 各 2 个

$|$3-cycle$| = 8$, $|H| \ge 8$ 舍

2. $\exists$ 3-cycle $\notin H$, 记为 x, $x^3 = 1 \in H$

$A_4/H = \{H, xH\}$, $x^2H = H$ or $x^2H = xH$ (舍)

$\therefore x^2H = H$ $\therefore x^2 \in H$ $(x^2)^{-1} = x \in H$ then $xH = H$ 矛盾

其实考虑 n-cycle 也可以, 只是 n=3 可行 比较好算

这个和 syl 有什么关系

HW3.18 $G \cong \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_{243}$ (1) # cyclic subgroup of order 9 $= \frac{\text{\# order 9 之元}}{\varphi(9)}$

(2) # non-cyclic subgroup of order 9

复习: Euler's Totient: $\gcd(x,n)=1$, $1 \le x \le n$, then $x^{\varphi(n)} \equiv 1 \pmod n$

$\varphi(n)$ 表示 $1, 2, \cdots n-1$ 中与 n 互质的个数

proof: 设 $G = \{r \in [1,n-1];\ \gcd(r,n)=1\}$, $\varphi(n)=|G|$ 群运算为 ⊗

G is group obv

$\forall a \in G$, $\langle a\rangle \le G$; $\exists m: a^m = e$; 故 $|\langle a\rangle| = m$

$|G| = |\langle a\rangle| \times |G:\langle a\rangle|$ $\therefore a^{\varphi(n)} = a^{|\langle a\rangle| + |G:\langle a\rangle|} = 1^{|G:\langle a\rangle|} = 1$

在 ⊗ = mod n 运算下 $a^{\varphi(n)} = 1$

即 $a^{\varphi(n)} \equiv 1 \pmod n$

(1) 在 G 中 order 为 9 的元素 $(a,b,c,d)^9 = (1,1,1,1)$; $(a,b,c,d)^8 \ne (1,1,1,1)$

$a^8 = 1$, $o(b), o(c), o(d)$ 中至少一个 order $=9$, 其余 1 或 3

3种 $\quad$ 1.3.9 $\quad$ 1.3.9 $\quad$ 1.3.9.243

$o(b,c,d) = (1,3,9) \ne (3,1,9), (1,1,9)$; $(9,1,3)\ (9,3,1)\ (9,1,1)$

$(1,9,3)\ (3,9,1)\ (1,9,1)$

$\begin{cases} (9,9,3)\ (9,9,1) \\ (9,1,9)\ (9,3,9) \ne (1,9,9)\ (3,9,9) \\ (9,9,9) \end{cases}$

$\mathbb{Z}_{243} = \{e, g, g^2, \cdots g^{243-1}\}$, $\quad g^{243} = 1$ $\therefore (g^{81})^3 = 1, (g^{-81})^3 = 1$

$(g^{162})^3 = 1, (g^{-162})^3 = 1$

阶只有 1.3.9.243, $\gcd(162, 243) \ne 1$, $\gcd(81, 243) \ne 1$ $\therefore g^{\pm 81}, g^{\pm 162}$ 阶 $=3$

$\Rightarrow \mathbb{Z}_{pq}$, $z^{pq} = 1$, $(z^p)^q = 1$ $\quad$ (z^p 代表 p 数字, $\mathbb{Z}_{pq} = z^0, z^1, \cdots z^{pq-1}$)

$\gcd(p, pq) = p \ne 1$ $\therefore z^p$ 的阶 $o(z^p) \mid q$

故 here $\mathbb{Z}_{243}$ 中 $\quad g^{\pm 81}, g^{\pm 162}$ $\quad o(\cdot) = 3$ $\quad$ 2个 (有重复 $g^{81} = g^{-162}$)

$g^{\pm 27}, g^{\pm 54}, g^{\pm 108}, g^{\pm 135}, \cancel{g^{\pm 162}}, g^{\pm 189}, g^{\pm 8\cdot 27}$, $\quad o(\cdot) = 9$ $\quad$ 6个

$\begin{cases} o(\cdot) = 3: & g^{243} = e \ \therefore (g^{81})^3 = e \quad 243 \div 81 - 1 = 2 \\ o(\cdot) = 9: & g^{243} = e \ \therefore (g^{27})^9 = e \quad 243 \div 27 - 1 - 2 = 6 \end{cases}$

(2): non-cyclic $G_9 \cong \mathbb{Z}_9$ 或 $\mathbb{Z}_3 \times \mathbb{Z}_3$ $\therefore$ 只有 $\mathbb{Z}_3 \times \mathbb{Z}_3 = \mathbb{Z}_3 \times \mathbb{Z}_3 \times 1 \times 1$ 列举