Algebra. Lec 8. Sylow theorem & application.

Thm. 6.4. $|G| = p^n \cdot m$. $(p, m) = 1$

① H: p-subgroup of G $\Rightarrow$ H is contained a p-Sylow

② all p-Sylow are conjugate

③ $Syl_p(G) \triangleq$ the set of all p-Sylow subgroups of G

$$n_p \triangleq |Syl_p(G)| \equiv 1 \pmod p$$

Rmk. ① if $n_p = |Syl_p(G)| = 1$.

$$|S| = 1 = \{P\}$$

i.e. $\forall g \in G$. $gPg^{-1} = P$ $\Rightarrow$ $P \trianglelefteq G$

Rmk. ② G finite p-group $\Rightarrow$ solvable

pf. class equation.

$$|G| = |Z(G)| + \underbrace{\sum_i (G : G_{x_i})}_{\text{divisible by } p.}$$

$\Rightarrow$ $Z(G)$ non-trivial.

$$G \supset Z(G) \supset \{e\}.$$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ G/Z(G) & \cdots & \{Z(G)\} \\ \downarrow & & \\ \text{by induction} & & \end{array} \implies \checkmark$$

Lem. 6.7. $|G|$. finite. p: smallest prime dividing $|G|$

$H \leq G$. $(G:H) = p \implies H \trianglelefteq G$

Pf. Let. $N_H = N \implies H \leq N \leq G$

则由 $(G:H) = p \implies N = G$ ✓ Lag.

or $N = H$

consider $N = H$. $|\text{the orbit of } H \text{ under conjugation}| = |\{gHg^{-1} \mid g \in G\}|$

G action

use G-action to understand. $= (G:N_H)$

$= p$

iso / hom

$G \longrightarrow \mathrm{Perm}(\{H_1, \dots, H_p\}) \cong S_p$

hom

$g \longmapsto \pi_g : H_i \longrightarrow gH_ig^{-1}$

$\ker(\varphi) = N_{H_1} \cap N_{H_2} \cap \cdots \cap N_{H_p}$

$$\begin{array}{c} \| \\ H \end{array}$$

$\Rightarrow \ker(\varphi) \leq H$

$$\left\{\begin{array}{ll} \ker(\varphi) = H & \Rightarrow \quad H \trianglelefteq G \\ \ker(\varphi) \underset{\neq}{\leq} H & \underbrace{(G : \ker\varphi) = \overbrace{(G:H)\,(H:\ker(\varphi)) = |\operatorname{im}(\varphi)|}^{1\text{st. iso}}}_{\text{Lag}} \;\Big|\; |S_p| \end{array}\right.$$

$\Rightarrow \quad p \cdot (H : \ker(\varphi)) \mid p!$

$(H : \ker(\varphi)) \mid (p-1)!$

$\Rightarrow$ get a prime factor in $(H : \ker(\varphi))$ $\square$

contradiction

Prop (application of Sylow)

p, q. distinct prime $|G| = pq \Rightarrow G$ solvable

Pf. let $p < q$. $\Rightarrow$ $P \in Syl_p(G)$ $\quad n_p = 1, 1+p, 1+2p, \ldots \quad n_p \mid q$

$Q \in Syl_q(G) \quad n_q = 1, 1+q, 1+2q \ldots \quad n_q \mid p$

$\Rightarrow n_q = 1$

$\Rightarrow Q \trianglelefteq G$

$$G = G_0 \supset \underbrace{Q}_{} \supset \{e\} \quad \Rightarrow \text{solvable}$$

$$\underbrace{G_0 \supset Q}_{G_0/Q} \quad \underbrace{Q \supset \{e\}}_{Q}$$

G_0/Q: p, cyclic Q: q, cyclic

eg. $|G| = 35 = 5 \times 7$. ($p < q$) $\Rightarrow$ G cyclic.

$H_5 \in Syl_5(G)$ $\quad n_5 = 1, 6, 11,$ $\quad n_5 \mid 7$

$H_7 \in Syl_7(G)$ $\quad n_7 = 1, 8, 15$ $\quad n_7 \mid 5$

$\Rightarrow n_5 = 1, n_7 = 1$

Consider. $H_5 \xrightarrow{\phi} Aut(H_7)$

$x \longmapsto \phi_x : H_7 \to H_7$

$y \mapsto xyx^{-1}$ $\to$ for $Syl_7(G)$ has only one element. so. $xH_7x^{-1} = H_7$

$\Rightarrow \phi_x \in Aut(H_7)$

$\Rightarrow im(\phi) \simeq H_5/_{ker(\phi)}$

$im(\phi) \leq Aut(H_7)$

$\Rightarrow |im(\phi)| \mid |Aut(H_7)|$ $\quad Aut(H_7) \simeq (\mathbb{Z}/7\mathbb{Z})^{\times} \simeq (\mathbb{Z}/6\mathbb{Z})$

$\Rightarrow |im(\phi)| \mid 6_{=q-1}$

$\Rightarrow |im(\phi)| = 1, 2, 3, 6 \quad \Rightarrow |im(\phi)| = 1 \Rightarrow \phi$: trivial ($p \nmid q-1$)

$\forall x \in H_5, y \in H_7 \quad xy = yx$

$$\begin{pmatrix} H_5 = \langle x \rangle \\ H_7 = \langle y \rangle \end{pmatrix}$$

Consider $\langle x \rangle \times \langle y \rangle \longrightarrow G$ hom.

$(x^{n_1}, y^{n_2}) \longmapsto (x^{n_1} y^{n_2})$ Surjective. and $|\langle x \rangle \times \langle y \rangle| = |G|$

$$\Rightarrow \quad \langle x \rangle \times \langle y \rangle \simeq G$$

$$\begin{array}{c} \wr\!\mid \\ (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z}) \simeq \mathbb{Z}/35\mathbb{Z} \end{array}$$

$\downarrow$

$(5,7) = 1$

G: cyclic

eg. $|G| = 2 \times 7$

$n_2 = 1, 3, 5, 7$, $\quad n_2 \mid 7 \quad \Rightarrow n_2 = 1, 7$

$n_7 = 1, 8, \ldots \quad n_7 \mid 2 \quad \Rightarrow n_7 = 1$

$\Rightarrow$ isomorphic classes of groups

① $\mathbb{Z}/14\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

②. D_{14}.

prime.

p^2

$p \times q$.

1 2 3 4 5 6 7 8 9 10 11

Δ

5 classes

finite abelian group.

[illegible]

12 13 14 15

Δ

Artin.

Conrad.

Solvable

(ex 27)

order < 60 solvable. $|A_5| = 60$ not solvable

for A_5 is simple

[1] • $\mathbb{Z}/p\mathbb{Z}$: cyclic $\overset{\text{(abelian)}}{\Longrightarrow}$ solvable.

[2] • $|G| = pq$. G : solvable.

[3] • G. p-group. G : solvable

[4] • $H \trianglelefteq G$ G : solvable $\iff$ G/H, H solvable.

[5] • $H \leq G$. G : solvable $\Longrightarrow$ H : solvable

(hint : normal tower of G. $G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$

$\Longrightarrow$ ~ of H. $H \cap G_0 \supset H \cap G_1 \supset \dots \supset \{e\}$)

[1] [2] [3] Do

1 2 3 4 5 6 7 8 9 10 11 12 ($2^2 \times 3$) ①

13 14 15 16 17 18 (2×3^2) ① 19 20 ($2^2 \times 5$) ① 21 22 23 24 ($2^3 \times 3$) ②

25 26 27 28 ($2^2 \times 7$) ① 29 30 ($2 \times 3 \times 5$) ③ 31 32 33 34 35 36 ($2^2 \times 3^2$) ②

37 38 39 40 ($2^3 \times 5$) ① 41 42 ($2 \times 3 \times 7$) ① 43 44 ($2^2 \times 11$) ① 45 46 47 48 ($2^4 \times 3$) ②

49 50 (2×5^2) ① 51 52 ($2^2 \times 13$) ① 53 54 (2×3^3) ① 55 56 ($2^3 \times 7$) 57 58 59 60

⓪ $G = \underbrace{S_4 \supset A_4}_{2} \underbrace{\supset \{e, (12)(34), (13)(24), (14)(23)\}}_{3} \underbrace{\supset \{e\}}_{4}$

i.e. S_4 is solvable

① $|G| = 28 = 2^2 \times 7$

$n_2 = 1, 7$ $\quad n_2 \mid 7$

$n_7 = 1,$ $\quad n_7 \mid 2$

$\Rightarrow n_2 = 1, 2, \; n_7 = 1 \Rightarrow \underset{\text{Syl}_7(G)}{Q} \trianglelefteq G \Rightarrow \underbrace{G \supset Q}_{4} \underbrace{\supset \{e\}}_{7}$

② $|G| = 12 = 2^2 \cdot 3$ $\quad \begin{cases} n_2 = 1, 3 \\ n_3 = 1, 4 \end{cases}$ $\quad$ if $n_2 = 1$ or $n_3 = 1$

$|G| = 24 = 2^3 \cdot 3$ $\quad \begin{cases} n_2 = 1, 3 \\ n_3 = 1, 4 \end{cases}$ $\quad \Rightarrow$ induction ✓

if $n_3 = 4$.

$G \xrightarrow{\phi} \text{Perm}(\text{Syl}_3(G)) \simeq S_4$

$g \longmapsto \pi_g : \text{Syl}_3(G) \to \text{Syl}_3(G)$ hom

$\qquad P \longmapsto gPg^{-1}$

$G/\ker(\phi) \simeq \text{im}(\phi) \leq S_4$ solvable

[5]

$\Rightarrow \text{im}(\phi)$ Solvable

and $\ker(\phi) \underset{\neq}{\leq} G \Rightarrow$ $G/\ker(\phi)$ solvable and $\ker(\phi)$ solvable $\overset{[4]}{\Rightarrow} G$ solvable

if $n_3 = 1$

$\text{Syl}_3(G) \ni Q \trianglelefteq G$

$\underbrace{G \supset Q}_{8} \underbrace{\supset \{e\}}_{3}$ ✓

$|G| = 2^4 \cdot 3$ $\left\{\begin{array}{l} n_2 = 1, 3 \\ n_3 = 1, 4, 16. \end{array}\right.$

if $n_2 = 3$.

Consider $G \xrightarrow{\phi} \mathrm{Perm}(\mathrm{Syl}_3(G)) \simeq S_3$

$g \mapsto \pi_g : \mathrm{Syl}_3(G) \to \mathrm{Syl}_3(G)$

$P \mapsto gPg^{-1}$

$\mathrm{im}(\phi) \trianglelefteq S_3$ solvable.

$\ker(\phi) \neq G$. $\Rightarrow$ $G/\ker(\phi) \simeq \mathrm{im}(\phi)$ solvable & $\ker(\phi)$ solvable. $\Rightarrow$ G solvable

① & ②

18. 2×3^2. $n_2 = 1, 3, \cancel{5}, \cancel{7}, 9$ $n_3 = 1, \cancel{4}$ by ①

20 $2^2 \times 5$. $n_2 = 1, \cancel{3}, 5,$ $n_5 = 1, \cancel{6}$ by ①

40 $2^3 \times 5$ $n_2 = 1, 5$ $n_5 = 1$ by ①

42. $2 \times 3 \times 7$. $n_2 = 1, 3, 7$

$n_3 = 1, 7$ by ①

$n_7 = 1$

44 $2^2 \times 11$ $n_2 = 1, 11$

by ①

$n_{11} = 1$

50 2×5^2 $n_2 = 1, 5, 25$

by ①

$n_5 = 1$

36 $2^2 \times 3^2$. $n_2 = 1, 3, 9$ if $n_3 = 4$.

by ②

$n_3 = 1, 4$. S_4 ✓

54. 2×3^3 $n_2 = 1, 3, 9, 27$

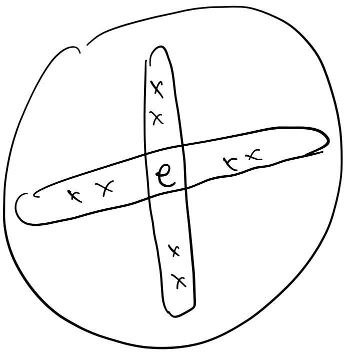
by ①

$n_3 = 1$

③ $|G|=30=2\times3\times5$

$$\begin{cases} n_2 = 1, 3, 5, 15 \\ n_3 = 1, 10 \\ n_5 = 1, 6 \end{cases}$$

if $n_5=6$.



by prop of cyclic groups

Counting: $(5-1)\times 6+1 = 25$

if $n_3=10 \Rightarrow$ too much elements $\Rightarrow n_3=1$ ✓

$|G|=56=2^3\times 7$

$n_2 = 1, 7$

$n_7 = 1, 8$

if $n_7=8$. $8\times(7-1)+1=49$

if $n_2\neq 1$

$|Q|=8$ $\Rightarrow$ too much elems. ✓

$\cap$

$Syl_2(G)$