Algebra Lec 7. sylow theorems

p. prime

- p-group. a finite group G. $|G| = p^n$
- $H \leq G$ $|H| = p^n$. H: p-subgroup of G
- $H \leq G$ $|G| = p^n \cdot m$. $(p, m) = 1$ $|H| = p^n$. H: p-Sylow subgroup.

Cauchy Theorem $|G| < \infty$. $p \mid |G|$

$$\Rightarrow \exists\, x \in G. \text{ s.t. } |x| = p.$$

$$\left(\langle x \rangle \leq G. \quad |\langle x \rangle| = p \right)$$

(Lem 6.1. special case of Cauchy)

Thm. 6.2. G. group. $|G| < \infty$. $p \mid |G|$.

$\Rightarrow \exists$ a p-Sylow subgroup of G

(i.e. $|G| = p^n \cdot m$. $(p, m) = 1$.

$\Rightarrow \exists H \leq G$. $|H| = p^n$.)

e.g. $|G| = 2^3 \cdot 3^2 = 72$

$\exists H_1 \leq G$. $|H_1| = 8$

$\exists H_2 \leq G$. $|H_2| = 9$.

---

pf. thm. 6.2

apply induction on the order of G

if $|G| = p$. done

∴ Assume the theorem holds for all groups of order $< |G|$

if. $\exists H \leq G$. s.t. $((G:H), p) = 1$. then done by induction.

(i.e $|H| = p^n \cdot k$, $|G| = p^n m$. $(m/k, p) = 1$)

now assume every subgroup of G have an index divisible by p.

$(G:H)$

$G \curvearrowright G$.

$G \times G \longrightarrow G$

$(g, x) \longrightarrow gxg^{-1}$

subgroup of G.

Class equation. $|G| = \underbrace{|Z(G)|} + \sum (G : G_x)$

divisible by p.

$\Rightarrow p \mid |Z(G)| \Rightarrow$ nontrivial center.

$\exists$ an element $\underset{Z(G)}{\underset{\cap}{a}}$ of order p. (by Cauchy thm)

$H = \langle a \rangle \leq Z(G) \leq G. \Rightarrow H \trianglelefteq G$

Let $f : \overset{p^n \cdot m}{G} \longrightarrow \overset{p^{n-1} m}{G/H}$.

$\qquad\qquad\qquad\qquad \rotatebox{90}{$\leq$}$

$\qquad\qquad\qquad\qquad \exists K' \quad |K'| = p^{n-1}$ (by induction)

$\Rightarrow \exists K \trianglelefteq f^{-1}(K')$

$K/H \simeq K'$ (1st. iso)

$\Rightarrow |K| = p^{n-1} \cdot p = p^n \qquad \square$

Rmk. class equation. application

Classify groups of order p^2, p: prime.

$$|G| = \underbrace{|Z(G)|}_{\text{divisible by } p} + \underbrace{\sum (G : G_x)}_{\text{divisible by } p} \qquad \overset{G_x \leq G}{\neq}$$

$\Rightarrow$ non trivial

$f: G \longrightarrow G/Z(G)$

order $= p^2$ order $= 1, p$.

$\Rightarrow G/Z(G)$. cyclic group. $G/Z(G) = \langle aZ(G) \rangle$

for some $a \in G$.

$\forall x, y \in G$ $x = a^{n_1} z_1$ $z_1, z_2 \in Z(G)$

$\downarrow$ $y = a^{n_2} z_2$

属于 some coset of $Z(G)$

so. $xy = a^{n_1+n_2}(z_1 z_2) = yx$. $\Rightarrow$ G is abelian. of order p^2

- if $\exists$ order p^2 element in G $\Rightarrow$ $G \cong \mathbb{Z}_{p^2} = \mathbb{Z}/p^2\mathbb{Z}$
- if $\nexists$ order p^2 element in G

$\Rightarrow$ i.e. every non-identity element have order p.

$\underbrace{\langle x \rangle}_{\text{order } p} \leq G$.   Consider $y \in G - \langle x \rangle$

$e \not\in$

$\Rightarrow |\langle y \rangle| = p$. $\langle y \rangle \leq G$

$\Rightarrow |\langle x, y \rangle| = p^2$ $\langle x, y \rangle \leq G \Rightarrow G = \langle x\ y \rangle$

Consider $\langle x \rangle \times \langle y \rangle \xrightarrow{\varphi} G$ $\Rightarrow$ hom

$$(x^{n_1}, y^{n_2}) \longmapsto x^{n_1} y^{n_2}$$

$$\langle x \rangle \times \langle y \rangle / \ker(\varphi) \simeq \mathrm{im}(\varphi) = G$$

$$\Rightarrow \boxed{G \simeq \mathbb{Z}_p \times \mathbb{Z}_p}$$

HW

[L]. chapter I ex 24 ex 25 ex 26 ex 28

ex 27.

Lemma. 6.3 H: p-group acting on a finite set S.

$\Rightarrow$ ⓐ (number of fixed points of H.) $\equiv |S| \pmod{p}$.

ⓑ if $\exists$ exactly 1 fixed point $\Rightarrow |S| \equiv 1 \pmod{p}$

ⓒ if $p \mid |S|$ (# of fixed pts) $\equiv 0 \pmod{p}$

<u>pf of ⓐ</u>

Orbit decomp. $\Rightarrow S = \bigsqcup (\text{orbits})$.

$$|S| = \sum |\text{orbit}|$$

$$= \sum (H : H_{x_i})$$

for a fixed point s. $hs = s$. $\forall h \in H$ i.e. $H = H_s$ $|H : H_s| = 1$

$$\Rightarrow |S| = \#\text{ of fixed points} + \boxed{\underset{(|\text{orbits}| \geq 2)}{\sum{}'} (H : H_{x_s})}$$

divisible by p.

$\Rightarrow$ ⓐ ✓ $\square$

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

① H : p-subgroup of G $\Rightarrow$ H is contained in some p-sylow subgroup.

② all p-sylow subgroups are conjugate

③ numbers of p-Sylow subgroup n_p. $n_p \equiv 1 \pmod p$

$$(n_p \mid m)$$

pf. Let P be a p-Sylow subgroup of G (by lemma 6.2)

Part I

Assume $H \leq N_P$. claim $H \subseteq P$

pf the claim. $H \leq N_P$, $P \leq N_P$ $\Rightarrow$ $HP/P \simeq H/H \cap P$

if $HP \neq P$ $\Rightarrow$ $|HP| = |P| \cdot |H/H \cap P|$ $\leftarrow$ pure power of p

$$|HP| > |P|$$

$\Rightarrow$ $\lightning$ contradiction.

$\therefore HP = P$

$\therefore H \subseteq P$

$S = \left(\begin{array}{l}\text{the set of all conjugates.} \\ \text{of } P \text{ in } G\end{array}\right) = \{ gPg^{-1} \mid g \in G \}$

$G \curvearrowright S$. only one orbit.

$$|S| = (G : G_P) = (G : N_P) \quad (P \leq N_P)$$

$m_P \mid m$

$\therefore |S|$: not divisible by p

Pf of ①

Let H be any p-subgroup of G. Then H acts on S by conjugation

$H \curvearrowright S$.

$|S| \equiv |\text{fixed points}| \pmod p$ (by lemma 6.3).

$\exists$ fixed points under H-action

Let Q be the fixed point $Q \in S$ (p-sylow)

i.e. $\forall h \in H$. $hQh^{-1} = Q$

$\Rightarrow H \leq N_Q$. by part I $\Rightarrow H \subseteq Q$ ◻

② follows from ① (P'. p-Sylow $\Rightarrow P'$ p-subgroup

$\Rightarrow P' \subset$ (some conjugates of P))

$\downarrow$
$=$

③

Q : p-Sylow

$Q \curvearrowright S \ni Q$

by part I, if $Q \leq N_{P_i} \Rightarrow Q = P_i$

then if $Q \neq P_i$, Q-action will move P_i around.

hence, Q is the only fixed point

$\Rightarrow S = \{Q\} \sqcup \{\text{other orbits}\}$

$\xRightarrow{\text{by lemma 6.3.}} \underset{\displaystyle n_p}{\overset{|S|}{\parallel}} \equiv \overset{\text{fixed point}}{1} \pmod p$