Abs. Alg #20 20^{03}_{27} 金

Thm 4.18 (Sylow's Theorem)

$|G| = p^\alpha m$, $p \nmid m$

(2)

$P \in Syl_p(G)$, $Q \leq G$: p-subg.

$\Rightarrow \exists g \in G$ s.t. $Q \leq gPg^{-1}$

とくに、

$Q \in Syl_p(G) \Rightarrow P \overset{conj.}{\sim} Q$

i.e. $\exists g \in G$. s.t. $Q = gPg^{-1}$.

(3)

$n_p \equiv 1 \pmod p$

さらに、

$\forall P \in Syl_p(G)$ $n_p = |G : N_G(P)|$

$n_p \mid m$

Date

2

★ (2) と (3) の証明の前に…

(1) より、G に対して $P \in Syl_p(G)$ が存在。そこで

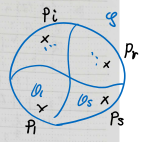
$\mathcal{S} := \{gPg^{-1} \mid g \in G\} = \{P_1, \cdots, P_r\}$

とし、$Q \leq G$: p-subgroup とする。$\mathcal{S}$ の定義より、

G は、したがって Q も、acts by conj. on $\mathcal{S}$.

Q の orbits $\mathcal{O}_1, \cdots, \mathcal{O}_s$ の union として $\mathcal{S}$ をかく：

$\mathcal{S} = \mathcal{O}_1 \sqcup \cdots \sqcup \mathcal{O}_s$



(ここで、$r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s|$

r は Q に依存しない。 $|\mathcal{O}_1| + \cdots + |\mathcal{O}_s|$ は Q に依存する。)

$\{P_1, \cdots, P_r\}$ の順序を必要に応じて変更し、最初の s コが

$\mathcal{O}_1, \cdots, \mathcal{O}_s$ の repr.s になるようにする：

$P_i \in \mathcal{O}_i$, $1 \leq i \leq s$.

* $P_i \in Syl_p(G)$

(∵) $c_{g_i} : P \to P_i = g_i P g_i^{-1}$

: bij.

∴ $|P_i| = |P| = p^\alpha$.

Prop 4.2 より、

$|\mathcal{O}_i| = |Q : N_Q(P_i)|$.

定義より、

$N_Q(P_i) = N_G(P_i) \cap Q$

Lem 4.19 より、*

$N_G(P_i) \cap Q = P_i \cap Q$

これらより、

$|\mathcal{O}_i| = |Q : P_i \cap Q|$, $1 \leq i \leq s$. (4.1)

3

▶ $r \equiv 1 \pmod p$ の証明.

Q は任意であったから、$Q = P_1$ とする。(4.1) より、

$|\mathcal{O}_1| = |P_1 : P_1| = 1$.

$1 < i$ ~~すう~~ について $P_1 \neq P_i$ ∴ $P_1 \cap P_i < P_1$. (4.1) より、

$|\mathcal{O}_i| = |P_1 : P_1 \cap P_i| > 1$, $2 \leq i \leq s$.

P_1 は p-group だから、*

$p \mid |P_1 : P_1 \cap P_i| = |\mathcal{O}_i|$.

∴ $r = |\mathcal{O}_1| + (|\mathcal{O}_2| + \cdots + |\mathcal{O}_s|)$

$\equiv 1 \pmod p$.

Date

$r \equiv 1 \pmod p$ $\mathcal{S} = \{gPg^{-1} \mid g \in G\} = \{P_1, \cdots, P_r\}$

4

$|Q| = p^\alpha$

▶ (2) (3) の証明.

(4.1)

$Q \leq G$: p-subg.

仮に $\forall i$ $Q \nleq P_i$ i.e. $\forall g \in G$ $Q \nleq gPg^{-1}$ とする.

このとき $\forall i$ $Q \cap P_i \boxed{<} Q$. ~~(4)~~ より、

$|\mathcal{O}_i| = |Q : Q \cap P_i| \boxed{>} 1$, $1 \leq i \leq s$.

$\forall i$ $p \mid |\mathcal{O}_i|$ であるから、$p \mid (|\mathcal{O}_1| + \cdots + |\mathcal{O}_s|) = r$. $p \mid r$

これは先に示した $r \equiv 1 \pmod p$ に矛盾. したがって、

$\exists g \in G$ s.t. $Q \leq gPg^{-1}$.

とくに、

$Q \in Syl_p(G)$ のとき、先の主張より、

$\exists g \in G$ s.t. $Q \leq gPg^{-1}$.

$|gPg^{-1}|$ ~~$= |Q|$~~ $= p^\alpha = |Q|$ であるから、$gPg^{-1} = Q$.

(2) が示せた.

とくに、$\mathcal{S} = Syl_p(G)$ (∵ $\forall Q \in Syl_p(G)$ $Q \overset{conj.}{\sim} P$) .

より、$n_p = r \equiv 1 \pmod p$

(3) の前半が示せた.

$\forall P, Q \in Syl_p(G)$, $P \overset{conj.}{\sim} Q$ と Prop 4.6 より、

$n_p = \# Syl_p(G) = |G : N_G(P)| = |G| / |N_G(P)|$

$p^\alpha m = |G| = n_p |N_G(P)|$, $|N_G(P)| \nmid m$ より、$n_p \mid m$.

(3) の後半が示せた.

5

☆ Note that…

Cor 4.14 とから、$\forall P, Q \in Syl_p(G)$ $P \cong Q$.