Sylow Theorems

七条 彰紀

2017 年 8 月 14 日

これは Keith Conrad 氏のノート "THE SYLOW THEOREMS" [†1] を元にした，Sylow の定理の証明とその応用についてのノートである．

定理 (Sylow Theorems)
任意の有限群 G について，その位数が素数 p，p に互いに素な正数 m，そして非負整数 n によって $|G| = p^n m$ と表されるとする．更に群 G の p-Sylow 部分群全体の集合を $\mathrm{Syl}_p(G)$ とおく．以下が成り立つ．

I. G は p-Sylow 部分群を持ち[†2]，またこれは G の任意の p-部分群を含む．
II. G の全ての p-Sylow 部分群は互いに共役である．
III. $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$
IV. 任意の p-Sylow 部分群 P について $|\mathrm{Syl}_p(G)| = [G : \mathrm{N}_G(P)]$
V. $|\mathrm{Syl}_p(G)|$ は m の約数である．

1 Prepares for The proof

群 G は集合 X に作用するものとする．この時，$g \in G, x \in X$ について，g が x に作用したものを（このセクションでは）$g * x$ で表す．

定義 1.1
安定化群 Stab_G，不変元の全体 Fix_G を以下で定める．

$$\mathrm{Stab}_G(X) = \{g \in G \mid g * x = x\}, \quad \mathrm{Fix}_G(X) = \{x \in X \mid {}^\forall g \in G, \ \ g * x = x\}.$$

また正規化群 N_G を部分集合 $S \subseteq G$ について次のように定める．

$$\mathrm{N}_G(S) = \{g \in G \mid gSg^{-1} = S\}.$$

$\mathrm{Stab}_G, \mathrm{N}_G$ がそれぞれ群であることは使う．また，$S \subseteq G$ が部分群である時に $\mathrm{N}_G(S)$ は S を正規部分群に持つ最大の部分群であることも（特に section 4 で）使う．

定理 1.2 (Orbit-Stabilizer Theorem)
群 G は集合 X に作用するものとする．以下が成り立つ．

$${}^\forall x \in X, \ \ |G/\mathrm{Stab}_G(x)| = |G * x|.$$

[†1] `http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/sylowpf.pdf`
[†2] すなわち $\mathrm{Syl}_p(G) \neq \emptyset$

(証明). 次の写像を考える（準同型とは限らない）.

$$\begin{array}{cccc} \phi: & G/\operatorname{Stab}_G(x) & \to & G * x \\ & g\operatorname{Stab}_G(x) & \mapsto & g * x \end{array}$$

明らかに ϕ は全射．あとは well-defined であることと単射であることを見れば良い．$g, h \in G$ を任意に取る．

$$\begin{aligned} & g * x = h * x \\ \iff & (h^{-1}g) * x = x \\ \iff & h^{-1}g \in \operatorname{Stab}_G(x) \\ \iff & (h^{-1}g)\operatorname{Stab}_G(x) = \operatorname{Stab}_G(x) \\ \iff & h^{-1}(g\operatorname{Stab}_G(x)) = \operatorname{Stab}_G(x) \\ \iff & g\operatorname{Stab}_G(x) = h\operatorname{Stab}_G(x) \end{aligned}$$

上から順に見ればこれは ϕ が単射であることの証明であり，下から順に見れば well-defined であることの証明になっている． ∎

定理 1.3 (Lagrange's Theorem)
任意の群 G とその部分群 U の位数について以下が成り立つ．

$$|G/U||U| = |G|.$$

これは $|G|, |U|$ が無限群であっても成り立つ．

(証明). この段落は『天書の証明』より引用する．二項関係

$$a \sim b \iff ba^{-1} \in U$$

を考える．群の公理から $\sim$ が同値関係であることがわかる．元 a を含む同値類はコセット

$$aU = \{ax \mid x \in U\}$$

に一致する．明らかに $|aU| = |U|$ なので，G は全ての大きさが $|U|$ である同値類に分解される．それゆえ，$|U|$ は $|G|$ を割る．

$$|G| = \sum_{i=1}^{|G/U|} |a_iU| = \sum_{i=1}^{|G/U|} |U| = |G/U||U|.$$

こうして主張の等式が得られる． ∎

補題 1.4 (Fixed Points Congurance)
群 G は集合 X に作用するものとする．$|G|$ が素数 p の倍数ならば，以下が成り立つ．

$$|X| \equiv |\operatorname{Fix}_G(X)| \mod p$$

(証明). X の G による軌道分解を考える．

$$X = \bigsqcup_{x \in X} Gx$$

すると Orbit-Stabilizer Theorem と Lagrange's Theorem より，

$$|X| = \sum_{x \in X} |G/\operatorname{Stab}_G(x)| = \sum_{x \in X} |G|/|\operatorname{Stab}_G(x)|$$

$\mathrm{Stab}_G(x)$ は G の部分群だから，$|\mathrm{Stab}_G(x)|$ も p の倍数か 1．したがって $|G|/|\mathrm{Stab}_G(x)|$ は p の倍数か 1 である．しかも $|G|/|\mathrm{Stab}_G(x)| = 1$ すなわち $\mathrm{Stab}_G(x) = G$ の時は $x \in \mathrm{Fix}_G(X)$ となっている．よって，$|X| = |\mathrm{Fix}_G(X)| + (p \text{ の倍数}) \equiv |\mathrm{Fix}_G(X)| \mod p$

∎

定理 1.5 (Cauchy's Group Theorem)
群 G の位数が p の倍数ならば，G は位数 p の巡回部分群を含む．

(証明). 位数 p の元の存在を示せば良い．この元は求める巡回群の生成元である．ここでは James H. McKay による論文 "Another Proof of Cauchy's Group Theorem" [†3] を紹介するに留める． ∎

2 Proof of Sylow Theorem I.

■整理と方針　ステートメントは定義から次のように論理式で表される．

$$^\forall i = 0, 1, \dots, n, \quad ^\exists H :: \text{subgroup of } G, \quad |H| = p^i$$

これを i に関する帰納法で証明しよう．まず，$i = 0$ の時は $H = \{e\}$ が条件を満たす．以下では $n > 0$ とし，$i = k < n$ の時 $|H| = p^k$ となる部分群 H が存在するならば，$H \subset H'$ かつ $|H'| = p^{k+1}$，すなわち $[H' : H] = p$ となる部分群 H' が存在することを示す．

■$\mathrm{Fix}_H(G/H)$ の定義．　中心となるアイデアは，集合 G/H の元であって，H による左からの積作用によって不変なものを考える，ということである．このような元全体を $\mathrm{Fix}_H(G/H)$ と置く．

$$\mathrm{Fix}_H(G/H) := \{gH \in G/H \mid {}^\forall h \in H, \ \ hgH = gH\}$$

■$\mathrm{Fix}_H(G/H) = \mathrm{N}_G(H)/H$．　この $\mathrm{Fix}_H(G/H)$ を別の表現にしよう．

$$\begin{aligned}
& gH \in \mathrm{Fix}_H(G/H) \\
\iff & {}^\forall h \in H, \ \ hgH = gH \\
\iff & {}^\forall h \in H, \ \ (g^{-1}hg)H = H \\
\iff & {}^\forall h \in H, \ \ (g^{-1}hg) \in H \\
\iff & g^{-1}Hg = H \\
\iff & g \in \mathrm{N}_G(H)
\end{aligned}$$

以上から，$\mathrm{Fix}_H(G/H) = \{gH \mid g \in \mathrm{N}_G(H)\} = \mathrm{N}_G(H)/H$ となる．$\mathrm{Fix}_H(G/H)$ が群だから，H は $\mathrm{N}_G(H)$ の正規部分群である．

■$\mathrm{N}_G(H)/H$ は p 群．　さて，補題から次が成り立つ．

$$|G/H| \equiv |\mathrm{Fix}_H(G/H)| \mod p$$

$k < n$ という条件と Lagrange's Theorem から，$|G/H| = |G|/|H| = p^{n-k}m$ は p の倍数．したがって $|\mathrm{Fix}_H(G/H)| = |\mathrm{N}_G(H)/H|$ も p の倍数．

[†3] `http://www.jstor.org/stable/2310010`

■Cauchy's Group Theorem から H' が存在． $|\mathrm{N}_G(H)/H|$ が p の倍数であるということは，Cauchy's Group Theorem から，$\mathrm{N}_G(H)/H$ は位数 p の巡回部分群を含む．それは群 $H' \subset \mathrm{N}_G(H)$ によって H'/H と表される．$|H'/H| = [H' : H] = p$ だから，帰納法が完成した．

3 Proof of Sylow Theorem II

■$\mathrm{Fix}_Q(G/P)$ は空でない． 群 G の p-Sylow 部分群 P,Q をとり，これらが共役であることを示す．Q は p-部分群なので以下が成り立つ．

$$|G/P| = [G : P] \equiv |\,\mathrm{Fix}_Q(G/P)| \mod p$$

$|P| = p^n$ から，$|G/P| = |G|/|P| = m$ は p の倍数でない．特に $|G/P| \equiv |\,\mathrm{Fix}_Q(G/P)| \not\equiv 0$ すなわち $\mathrm{Fix}_Q(G/P)$ は空集合でない．

■$\mathrm{Fix}_Q(G/P)$ の元の定義から結論へ． $\mathrm{Fix}_Q(G/P)$ の元を一つ取って gP とおく．定義から，全ての Q の元 q に対して

$$qg \cdot P = gP \implies qg \cdot e \in gP \iff qg \in gP \iff Q \subset gPg^{-1}$$

となる．P, Q はどちらも p-Sylow 部分群で，位数は同じ．したがって $Q = gPg^{-1}$

4 Proof of Sylow Theorem III

■方針． $\mathrm{Syl}_p(G)$ の元を一つとり P とする．そして集合 $\mathrm{Syl}_p(G)$ への P の共役作用を考える．P は p-部分群なので，

$$|\,\mathrm{Syl}_p(G)| \equiv |\,\mathrm{Fix}_P(\mathrm{Syl}_p(G))| \mod p.$$

以下で $|\,\mathrm{Fix}_P(\mathrm{Syl}_p(G))| = 1$ を示す．

■不動点 Q を取る． $\mathrm{Fix}_P(\mathrm{Syl}_p(G))$ に P が属すことは，任意の $p \in P$ について $p^{-1}Pp = P$ であることから自明．なので $\mathrm{Fix}_P(\mathrm{Syl}_p(G))$ からもうひとつ元をとって Q とする．

■$P, Q, \mathrm{N}_G(Q)$ の関係． この時，$P, Q \subset \mathrm{N}_G(Q) \subset G$ だから[†4]，位数を考えれば $P, Q \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$ も成り立つ．また，Q は $\mathrm{N}_G(Q)$ の正規部分群（Sylow Theorem I でも触れた）である．

■$P = Q$ を示す． Sylow Theorem II から P, Q は $\mathrm{N}_G(Q)$ の部分群として互いに共役．ところが正規部分群の定義より，$\mathrm{N}_G(Q)$ の部分群で Q と共役なものは Q 自身しか無い．よって $P = Q$ となり，$\mathrm{Fix}_P(\mathrm{Syl}_p(G)) = \{P\}$ が示された．

5 Proof of Sylow Theorem IV

Orbit-Stabilizer Theorem を集合 $\mathrm{Syl}_p(G)$ とこれに共役作用する群 G に用いる．Sylow Theorem II から $\mathrm{Syl}_p(G)$ の元は互いに共役だから，G の共役作用による軌道は一つしか無い．

$${}^\forall P \in \mathrm{Syl}_p(G), \quad |G/\,\mathrm{Stab}_G(P)| = |G * P| = |\,\mathrm{Syl}_p(G)|.$$

[†4] 念の為．$\mathrm{N}_G(Q) := \{g \in G \mid g^{-1}Qg = Q\}$ であり，$Q \in \mathrm{Fix}_P(\mathrm{Syl}_p(G))$ から任意の $p \in P$ について $p^{-1}Qp = Q$ が成立する．

$\mathrm{Stab}_G(P) = \{g \in G \mid g^{-1}Pg = P\} = \mathrm{N}_G(P)$ なので，

$$^{\forall}P \in \mathrm{Syl}_p(G),\ \ |\mathrm{Syl}_p(G)| = [G : \mathrm{N}_G(P)].$$

6 Proof of Sylow Theorem V

Sylow Theorem V から $|\mathrm{Syl}_p(G)|$ は素数 p と互いに素．また，Sylow Theorem IV と Lagrange's Theorem から $|\mathrm{Syl}_p(G)| = [G : \mathrm{N}_G(P)] = |G|/|\mathrm{N}_G(P)|$ なので $|\mathrm{Syl}_p(G)|$ は $|G| = p^n m$ の約数である．よって $|\mathrm{Syl}_p(G)|$ は m の約数.

7 Applications

補題 7.1 (Frattini's Argument)
H を群 G の正規部分群，P を H の p-Syllow 部分群とすると，$G = \mathrm{N}_G(P)H$ である．

(証明). $H, \mathrm{N}_G(H) \subseteq G$ から $G \supseteq \mathrm{N}_G(P)H$．逆の包含関係を示す．$G$ の任意の元 g を取る．H は G の正規部分群だから，

$$g^{-1}Pg \subset g^{-1}Hg = H$$

したがって $g^{-1}Pg$ も H の p-Syllow 部分群である．すると Sylow Theorem II より，ある $h \in H$ が存在して

$$hg^{-1}Pgh^{-1} = (gh^{-1})^{-1}Pgh^{-1} = P.$$

$\mathrm{N}_G(P)$ の定義から，$gh^{-1} \in \mathrm{N}_G(P)$．よって $g \in \mathrm{N}_G(P)H$ が成立. ∎

命題 7.2 (Sylow's test)
n を素数でない正の整数とし，p を n の素因数とする．もし n の約数の中で p を法として 1 と合同なものが 1 のみであれば，位数 n の単純群は存在しない．

(証明). 位数 n の任意の群を G とする．n が素数の冪数ならば G は非自明な中心を持つ．したがって単純群でない．

n は素数の冪数でないとする．すると G の任意の p-Sylow 群は真部分群である．すなわち $\mathrm{Syl}_p(G) \not\ni G$ である．そして Sylow Theorem III より $|\mathrm{Syl}_p(G)| \mod p = 1$ であるが，Sylow Theorem V と仮定から，このような $|\mathrm{Syl}_p(G)|$ は 1 しか無い．よって G の p-Sylow 部分群は唯 1 つであり，$\mathrm{Syl}_p(G) \not\ni G$ と Sylow Theorem II から，これは G の正規部分群．よって G は単純群でない． ∎