

# Sylow Theorems

七条 彰紀

平成 28 年 8 月 2 日

これは Keith Conrad 氏のノート “THE SYLOW THEOREMS”<sup>1)</sup> 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 0.1** (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  $\text{Syl}_p(G)$  とおく。以下が成り立つ。

- I.  $G$  は  $p$ -Sylow 部分群を持ち<sup>2)</sup>、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.  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$
- IV. 任意の  $p$ -Sylow 部分群  $P$  について  $|\text{Syl}_p(G)| = [G : N_G(P)]$
- V.  $|\text{Syl}_p(G)|$  は  $m$  の約数である。

## 1 Prepares for The proof

**定理 1.1** (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。

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

3)

(証明). 任意の  $g, h \in G$  を取る。

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

よって  $g * \text{Stab}_G(x) \mapsto g * x$  は全単射。 ■

<sup>1)</sup><http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/sylowpf.pdf>

<sup>2)</sup>すなわち  $\text{Syl}_p(G) \neq \emptyset$

<sup>3)</sup> $\text{Stab}_G(x) := \{g \in G : g * x = x\}$

**定理 1.2** (Lagrange's Theorem). 任意の有限群  $G$  とその部分群  $U$  の位数について以下が成り立つ。

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

(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

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

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。

あとは

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

より、最終的な等式が成り立つ。

■

**補題 1.3** (Fixed Points Congruance). 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。

$$|X| \equiv |\text{Fix}_G(X)| \pmod{p}$$

4)

(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、

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

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

■

**定理 1.4** (Cauchy's Group Theorem). 群  $G$  の位数が  $p$  の倍数ならば、 $G$  は位数  $p$  の巡回群を含む。

(証明). 位数  $p$  の元の存在を示す。この元は求める巡回群の生成元である。 ■

<sup>4)</sup>  $\text{Fix}_G(X) := \{x \in X : \forall g \in G, g * x = x\}$

## 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。

$$\forall i \in [0, n], \exists H : \text{a group s.t. } H \subset G \wedge |H| = p^i$$

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。

$\text{Fix}_H(G/H)$  の定義 中心となるアイデアは、集合  $G/H$  の元で、 $H$  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  $\text{Fix}_H(G/H)$  と置く。

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

$\text{Fix}_H(G/H) = N_G(H)/H$  この  $\text{Fix}_H(G/H)$  を別の表現にしよう。

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

ただし  $N_G(H)$  は正規化群で  $N_G(H) := \{g \in G : g^{-1}Hg = H\}$  である。途中で  $h \mapsto g^{-1}hg$  が全単射だから集合として  $|g^{-1}Hg| = |H|$ 、ということを用いた。以上から、 $\text{Fix}_H(G/H) = \{gH : g \in N_G(H)\} = N_G(H)/H$  となる。 $\text{Fix}_H(G/H)$  が群だから、 $H$  は  $N_G(H)$  の正規部分群である。

$N_G(H)/H$  は  $p$  群 さて、補題から次が成り立つ。

$$|G/H| \equiv |\text{Fix}_H(G/H)| \pmod{p}$$

$k < n$  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  $|\text{Fix}_H(G/H)| = |N_G(H)/H|$  も  $p$  の倍数。

Cauchy's Group Theorem から  $H'$  が存在  $|N_G(H)/H|$  が  $p$  の倍数であるということは、Cauchy's Group Theorem から、これは位数  $p$  の巡回群を持つ。それは群  $H' \subset N_G(H)$  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

Fix<sub>Q</sub>(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。使うのはやはり Fixed Points Congurance だ。  $Q$  は  $p$ -部分群なので以下が成り立つ。

$$|G/P| = [G : P] \equiv |\text{Fix}_Q(G/P)| \pmod{p}$$

$|P| = p^n$  から、  $|G/P| = |G|/|P| = m$  は  $p$  の倍数でない。したがって  $\text{Fix}_Q(G/P) = \{gP \in G/P : \forall q \in Q, qgP = gP\}$  は空集合でない。

Fix<sub>Q</sub>(G/P) の元の定義から結論へ  $\text{Fix}_Q(G/P)$  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  $\text{Syl}_p(G)$  の元を一つとり  $P$  とする。そして集合  $\text{Syl}_p(G)$  への  $P$  の共役作用を考える。  $P$  は  $p$ -部分群なので、ここでも Fixed Points Congurance を使える。

$$|\text{Syl}_p(G)| \equiv |\text{Fix}_P(\text{Syl}_p(G))| \pmod{p}$$

以下で  $|\text{Fix}_P(\text{Syl}_p(G))| = 1$  を示す。

不動点  $Q$  を取る  $\text{Fix}_P(\text{Syl}_p(G))$  に  $P$  が属すことは  $\forall p \in P, p^{-1}Pp = P$  から自明なので、  $\text{Fix}_P(\text{Syl}_p(G))$  からもうひとつ元をとって  $Q$  とする。

$P, Q, N_G(Q)$  の関係 この時、  $P, Q \subset N_G(Q) \subset G$  だから<sup>5)</sup>、位数を考えれば  $P, Q \in \text{Syl}_p(N_G(Q))$  も成り立つ。また、  $Q$  は  $N_G(Q)$  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  $N_G(Q)$  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、  $N_G(Q)$  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、  $\text{Fix}_P(\text{Syl}_p(G)) = \{P\}$  が示された。

<sup>5)</sup>念の為。  $N_G(Q) := \{g \in G : g^{-1}Qg = Q\}$  であり、  $Q \in \text{Fix}_P(\text{Syl}_p(G))$  から  $\forall g \in P, g^{-1}Qg = Q$  が成立する。

## 5 proof of Sylow Theorem IV

Orbit-Stabilizer Theorem を集合  $\text{Syl}_p(G)$  とこれに共役作用する群  $G$  に用いる。Sylow Theorem II から  $\text{Syl}_p(G)$  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。

$$\forall P \in \text{Syl}_p(G), |G/\text{Stab}_G(P)| = |G * P| = |\text{Syl}_p(G)|$$

$\text{Stab}_G(P) = \{g \in G : g^{-1}Pg = P\} = N_G(P)$  なので、

$$\forall P \in \text{Syl}_p(G), |\text{Syl}_p(G)| = [G : N_G(P)]$$

## 6 proof of Sylow Theorem V

Sylow Theorem V から  $|\text{Syl}_p(G)|$  は素数  $p$  と互いに素。また、Sylow Theorem IV と Lagrange's Theorem から  $|\text{Syl}_p(G)| = [G : N_G(P)] = |G|/|N_G(P)|$  なので  $|\text{Syl}_p(G)|$  は  $|G| = p^n m$  の約数である。よって  $|\text{Syl}_p(G)|$  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  $p$ -Sylow 部分群とすると、 $G = N_G(P)H$  である。

(証明).  $G$  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  $p$ -Sylow 部分群である。すると Sylow Theorem II より、ある  $h \in H$  が存在して

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

$N_G(P)$  の定義から、 $gh^{-1} \in N_G(P)$ 。よって  $g \in N_G(P)H$  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  $\text{Syl}_p(G) \not\cong G$  である。そして Sylow Theorem III より  $|\text{Syl}_p(G)|$

$\text{mod } p = 1$  であるが、Sylow Theorem V と仮定から、このような  $|\text{Syl}_p(G)|$  は 1 しか無い。よって  $G$  の  $p$ -Sylow 部分群は唯 1 つであり、 $\text{Syl}_p(G) \not\cong G$  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。 ■