1 共役集合の個数

G を群とする. G の部分集合 S と G の元 g に対して, G の部分集合

$$gSg^{-1} = \{gxg^{-1} \mid x \in S\}$$

を S の g による共役集合という. 特に, S が G の部分群であるとき, gSg^{-1} もまた G の部分群であり, S と同型である. このとき, gSg^{-1} を S の g による共役部分群という.

G の部分集合 S, S' について, S' が G において S と共役 (conjugate) であるとは, ある $g \in G$ が存在して $S' = gSg^{-1}$ となるときにいう. またこのとき, S' は G における S の共役集合であるという. S, S' が G の部分群であるとき[1)]は, S' は G における S の共役部分群であるという.

［定理 1.1］ G を群, S を G の部分集合とし, G の $N_G(S)$ による左剰余類の全体を $G/N_G(S)$ と書く. ただし, $N_G(S)$ は S の正規化群 (normalizer) である:

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

また, S の共役集合の全体からなる集合を $\mathcal{M}$ とおく:

$$\mathcal{M} = \{gSg^{-1} \mid g \in G\}.$$

このとき, 全単射

$$f : G/N_G(S) \to \mathcal{M}, \quad gN_G(S) \mapsto gSg^{-1}$$

が存在する.

［証明］ $\mathfrak{P}(G)$ を G の部分集合全体からなる集合とする.

$$G \times \mathfrak{P}(G) \to \mathfrak{P}(G), \quad (g, S) \mapsto g \circ S = gSg^{-1}$$

は G の $\mathfrak{P}(G)$ への作用である. $S \in \mathfrak{P}(G)$ に対し, S の軌道は

$$\mathrm{Orb}_G(S) = \{g \circ S \mid g \in G\} = \mathcal{M}$$

であり, S の固定群は

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

である. このとき, 全単射

$$G/\mathrm{Stab}_G(S) \to \mathrm{Orb}_G(S), \quad g\,\mathrm{Stab}_G(S) \mapsto g \circ S$$

が存在する. □

[1)] S' が G において S と共役であるとき, S, S' の一方が G の部分群ならばもう一方も G の部分群である.

［系 1.2］ G を有限群, S を G を部分集合とする．このとき, G における S の共役集合の個数は $(G : N_G(S))$ である．

群 G の元 x, g に対して, G の元 gxg^{-1} を x の g による共役元という．gxg^{-1} の位数は x の位数と一致する．

G の元 x, x' について, x' が G において x と共役 (conjugate) であるとは, ある $g \in G$ が存在して $x' = gxg^{-1}$ となるときにいう．またこのとき, x' は G における x の共役元であるという．

G における x の共役元全体からなる G の部分集合 $\{gxg^{-1} \mid g \in G\}$ を, x を含む G の共役類 (conjugacy class) という．

［系 1.3］ G を有限群, x を G の元とする． このとき, x を含む G の共役類の元の個数[2)]は $(G : N_G(x))$ である．

［証明］ x を含む G の共役類と, 1 元集合 $\{x\}$ の G における共役集合の全体との間には自明な 1 対 1 対応があることに注意して, $S = \{x\}$ として系 1.2 を適用せよ． $\square$

［定理 1.4（類等式）］ G を有限群とする．2 つ以上の元を含む G の共役類のすべてを C_1, C_2, ..., C_s とする．このとき, 等式

$$|G| = |Z(G)| + \sum_{i=1}^{s} |C_i|$$

が成り立つ．これを類等式 (class equation or class formula) という．ただし, $Z(G)$ は G の中心 (center) である:

$$Z(G) = \{x \in G \mid xg = gx \ (\forall g \in G)\}.$$

［証明］ G の 2 つの元が共役であるという関係は G 上の同値関係である．この同値関係による同値類が G の共役類である．よって, G は各共役類の集合としての直和で表される．ゆえに, $|G|$ は各共役類の元の個数の和に等しい．すなわち,

$$|G| = \sum_{|C|=1} |C| + \sum_{i=1}^{s} |C_i|.$$

ここで, C は元の個数が 1 つしかない G の共役類全体をわたる．

さて, $x \in G$ に対し, x が属する共役類を $C(x)$ と書く．全単射

$$\{x \in G \mid |C(x)| = 1\} \to \{C \mid |C| = 1\}, \quad x \mapsto \{x\}$$

[2)] すなわち, G における x の共役元の個数．

が存在するから,

$$\begin{aligned}\sum_{|C|=1}|C| &= \sum_{C\in\{C||C|=1\}}|C| = \sum_{C\in\{C||C|=1\}}1\\ &= \#\{C \mid |C|=1\}\\ &= \#\{x\in G \mid |C(x)|=1\}.\end{aligned}$$

さらに, $x \in G$ について,

$$\begin{aligned}|C(x)|=1 &\iff C(x)=\{x\}\\ &\iff gxg^{-1}=x\ (\forall g\in G)\\ &\iff gx=xg\ (\forall g\in G)\end{aligned}$$

であるから,

$$\{x\in G \mid |C(x)|=1\}=Z(G).$$

したがって, 求める等式が得られる. □

2 群論における Cauchy の定理

［補題 2.1］ G, G' を群, $f: G\to G'$ を準同型写像, a を G の有限位数の元とする. このとき, $f(a)$ の位数は a の位数の約数である.

［証明］ G, G' の単位元をそれぞれ e, e' とおく. a の位数を n とすると, $a^n=e$ であるから,

$$f(a)^n=f(a^n)=f(e)=e'.$$

よって, $f(a)$ の位数は n の約数である. □

［補題 2.2］ G を有限 Abel 群, p を素数とし, G の位数 $|G|$ は p で割れるものとする. このとき, G は位数 p の元を含む.

［証明］ $|G|=pm$ とおく. m に関する数学的帰納法により証明する.

$m=1$ のとき, $|G|=p>1$ より G の単位元以外の元 a が存在する. a の位数は, $|G|=p$ の約数であるから, 1 または p である. ところが, 位数が 1 の元は単位元しかない. よって, a の位数は p である.

$m-1$ まで補題の主張が正しいと仮定する. $x\in G$ を単位元以外の元とし, x の位数を n とおく. x は単位元でないから, $n>1$ である.

n が p の倍数のとき, $x^{n/p}$ の位数は p である.

n が p の倍数でないとき, G は Abel 群なので, 剰余群 $G/\langle x\rangle$ もまた Abel 群であって,

$$|G/\langle x\rangle| = \frac{|G|}{|\langle x\rangle|} = \frac{pm}{n}.$$

$|G/\langle x\rangle|$ は整数なので n は pm を割るが, n は p の倍数でないという仮定から, n は m を割る. すなわち, m/n は整数である. ゆえに, $|G/\langle x\rangle|$ は p の倍数である. しかも, $m/n < m$ である. 帰納法の仮定より, $G/\langle x\rangle$ は位数 p の元をもつ. したがって, $\pi : G \to G/\langle x\rangle$ を自然な全射準同型とすると, ある $y \in G$ が存在して $\pi(y)$ は $G/\langle x\rangle$ の位数 p の元である. y の位数を n' とおくと, 補題 2.1 より n' は p の倍数である. そして, $y^{n'/p}$ の位数は p である.

以上より, すべての m に関して, 補題の主張は正しい. □

［補題 2.3］ G を有限群, p を素数とし, G の任意の固有の部分群[3] H に対して

$$(G : H) \equiv 0 \pmod p$$

が成り立つとする. このとき, G の中心 $Z(G)$ の位数は p の倍数である.

［証明］ 2 つ以上の元を含む G の共役類のすべてを $C_1, C_2, \ldots, C_s$ とすると, 定理 1.4 より, 類等式

$$|G| = |Z(G)| + \sum_{i=1}^{s}|C_i|$$

が成り立つ. また, 各番号 i に対して, x_i を C_i の代表元, $N_G(x_i)$ を x_i の正規化群とすると, 系 1.3 より,

$$(G : N_G(x_i)) = |C_i| > 1.$$

よって, $N_G(x_i) \neq G$ である. 仮定より,

$$|C_i| = (G : N_G(x_i)) \equiv 0 \pmod p.$$

一方, 仮定より,

$$|G| = (G : \{e\}) \equiv 0 \pmod p.$$

したがって, $|Z(G)| \equiv 0 \pmod p$ が成り立つ. □

［系 2.4］ G を有限群, p を素数とし, G の位数は p の冪であるとする. このとき, G の中心 $Z(G)$ の位数は p の倍数である.

[3] 群 G の部分群 H で $H \neq G$ なるものを固有の部分群 (proper subgroup) という.

［**証明**］G の任意の部分群 H に対して, $H \neq G$ ならば,

$$|G| = (G:H) \cdot |H|, \quad (G:H) > 1$$

が成り立つ. すなわち, $(G:H)$ は $|G|$ の 1 より大きい約数である. $|G|$ は p の冪だから, $(G:H)$ は p の倍数である. $\square$

［**補題 2.5**］G を群, $Z(G)$ を G の中心, N を $Z(G)$ の部分群とする. このとき, N は G の正規部分群である.

［**証明**］最初に, $Z(G)$ は G の部分群だから, N は G の部分群である. $x \in N$, $g \in G$ を任意にとる. $N \subseteq Z(G)$ より $x \in Z(G)$ であるから, $gx = xg$. すなわち, $gxg^{-1} = x \in N$. したがって, N は G の正規部分群である. $\square$

［**補題 2.6**］G を群とし, N を G の正規部分群とする. G/N を G の N による剰余群とし, $\mathcal{K}$ を G/N の部分群とする. このとき, G のある部分群 K が存在して, $K/N \cong \mathcal{K}$ が成り立つ.

［**証明**］$\pi : G \to G/N$ を自然な全射準同型とする. $K = \pi^{-1}(\mathcal{K})$ は G の部分群であり, $N \subseteq K$ が成り立つ. 一方, π の K への制限

$$\pi_K : K \to G/N, \quad x \mapsto \pi(x)$$

を考えると, $\pi_K : K \to \pi(K) = \mathcal{K}$ は全射準同型であり,

$$\ker(\pi_K) = K \cap N = N.$$

したがって, 準同型定理により, 同型

$$K/N \cong \mathcal{K}, \quad xN \mapsto \pi(x)$$

が得られる. $\square$

［**定理 2.7**］G を有限群, p を素数, $k \geq 0$ を整数とし, G の位数は p^k で割れるものとする. このとき, G は位数 p^k の部分群を含む.

［**証明**］G の位数 $|G|$ に関する数学的帰納法により証明する.

$|G| = 1$ のとき, G は単位元のみからなる群 $\{e\}$ であり, G 自身が位数 $p^0 = 1$ の部分群である. したがって, 定理は成り立つ.

$|G| > 1$ のとき, $|G|$ より小さな位数の有限群に対しては定理が成り立つと仮定する.

G のある固有の部分群 H が存在して $(G:H) \not\equiv 0 \pmod p$ が成り立つ場合, $|G| = (G:H) \cdot |H|$ より $|H|$ が p^k で割り切れる．帰納法の仮定より $|H|$ は位数 p^k の部分群を含む．それは G の部分群でもある．

G のすべての固有の部分群 H に対して $(G:H) \not\equiv 0 \pmod p$ が成り立つ場合, 補題 2.3 より G の中心 $Z(G)$ の位数は p の倍数である．$Z(G)$ は Abel 群だから, 補題 2.2 より $Z(G)$ は位数 p の元をもつ．その元で生成される $Z(G)$ の位数 p の部分群を N とする．補題 2.5 より N は G の正規部分群である．よって, 剰余群 G/N が定まる．その位数について

$$|G/N| = \frac{|G|}{|N|} = \frac{|G|}{p}$$

が成り立つから, $|G/N| < |G|$ であり, かつ $|G/N|$ は p^{k-1} の倍数である．帰納法の仮定より, G/N の部分群 $\mathcal{K}$ で $|\mathcal{K}| = p^{k-1}$ なるものが存在する．補題 2.6 より, G の部分群 K が存在して, 同型 $K/N \cong \mathcal{K}$ が成り立つ．このとき,

$$\frac{|K|}{p} = \frac{|K|}{|N|} = |K/N| = |\mathcal{K}| = p^{k-1}.$$

これより, $|K| = p^k$ を得る．

以上より, すべての有限群 G に対して, 定理の主張は正しい． □

［**系 2.8（Cauchy の定理）**］G を有限群, p を素数とし, G の位数は p で割れるものとする．このとき, G は位数 p の元を含む．

［**証明**］定理 2.7 より, G の位数 p の部分群 K が存在する．$|K| = p > 1$ より, K の単位元以外の元 a が存在する．言うまでもなく a は G の元である．a の位数は, $|K| = p$ の約数であるから, 1 または p である．ところが, 位数が 1 の元は単位元しかない．よって, a の位数は p である． □

3 Sylow の定理

有限群 G の部分群の位数は必ず G の位数の約数である．逆は一般には成立しないが, G の位数を割る素数冪 p^l に対しては, 位数 p^l の部分群は必ず存在する．特に, G の位数を割る素数 p の冪で最大のものを位数とする部分群のことを Sylow p 部分群という．Sylow の定理 (Sylow theorems) と呼ばれるいくつかの定理は, Sylow p 部分群の存在と性質について述べたもので, 有限群論において基本的である．

G を有限群, p を素数とする．

G の部分群で, すべての元の位数が p の冪であるものを, G の p 部分群 (p-subgroup) という．さらに, G の位数 $|G|$ を素因数分解すると, 整数 $l \geq 0$ と整数 $m \geq 1$ が一意的に存在して,

$$|G| = p^l m, \quad \gcd(p, m) = 1$$

と表すことができる. G の位数 p^l の部分群を G の Sylow p 部分群 (Sylow p-subgroup) という[4].

［定理 3.1（Sylow の定理）］ G を有限群, p を素数とする. このとき, G の Sylow p 部分群が少なくとも 1 つ存在する.

［証明］ 定理 2.7 より明らか. □

［命題 3.2］ G を有限群, p を素数とする. G の Sylow p 部分群は, G の p 部分群のうちで包含関係について極大なものである.

［証明］ P を G の Sylow p 部分群, H を G の p 部分群とし, $P \subseteq H$ であるとすると, $|P| \leq |H|$ である. また, 整数 $l \geq 0$ と整数 $m \geq 1$ によって

$$|G| = p^l m, \quad \gcd(p, m) = 1$$

と表すとき, Sylow p 部分群の定義より P の位数は p^l であり, H の位数は, $|G|$ の約数であるが, $\gcd(p, m) = 1$ より p^l の約数になる. ゆえに, $|H| \leq |P|$. したがって, $|H| = |P|$ となり, $P = H$ がいえる. □

［命題 3.3］ G を有限群, p を素数とする. G の Sylow p 部分群の G における共役部分群もまた G の Sylow p 部分群である.

［証明］ 一般に, G において共役な 2 つの部分群は同型であり, 特に位数が一致する. よって, G の Sylow p 部分群 P の G における共役部分群 P' の位数は P の位数と同じである. ゆえに, P' もまた G の Sylow p 部分群である. □

［補題 3.4］ G を群, H, K を G の部分群とし, $H \subseteq N_G(K)$ であるとする. このとき, $HK = KH$ であり, かつ HK は G の部分群である.

［証明］ 任意の $h \in H, k \in K$ に対して, $H \subseteq N_G(K)$ という仮定より,

$$hk = (hkh^{-1})h \in KH.$$

ゆえに, $HK \subseteq KH$. 逆に, 任意の $h \in H, k \in K$ に対して, 再び $H \subseteq N_G(K)$ という仮定より,

$$kh = h(h^{-1}kh) = h(h^{-1}k(h^{-1})^{-1}) \in HK.$$

ゆえに, $KH \subseteq HK$. したがって, $HK = KH$ である.

[4] 素数 p が $|G|$ を割らないとき, G の Sylow p 部分群は単位元のみからなる群である.

H, K はともに単位元 e を含むので, HK もまた単位元 e を含む. よって, HK は空集合ではない. さらに,

$$(HK)(HK) = H(KH)K = HHKK = HK,$$
$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK.$$

ゆえに, HK は G の部分群である. □

［補題 3.5］ G を有限群, p を素数, P を G の Sylow p 部分群, H を G の p 部分群とする. このとき,

$$H \subseteq N_G(P) \iff H \subseteq P$$

が成り立つ.

［証明］ ($\Rightarrow$) $H \subseteq N_G(P)$ と仮定すると, 補題 3.4 より, HP は G の部分群である. また,

$$|HP| = \frac{|H| \cdot |P|}{|H \cap P|}$$

であり, $|H|$, $|P|$ はともに p の冪であるから, $|HP|$ もまた p の冪である. よって, HP は G の p 部分群である. しかも, $P \subseteq HP$ であり, P は G の Sylow p 部分群であるから, $HP = P$. これと $H \subseteq HP$ より, $H \subseteq P$.

($\Leftarrow$) $H \subseteq P$ と仮定すると, $P \subseteq N_G(P)$ より, $H \subseteq N_G(P)$. □

［補題 3.6］ G を有限群, p を素数とする. P を G の Sylow p 部分群とし, P の G における共役部分群の全体からなる集合を $\mathrm{Conj}(P)$ とおく. すなわち,

$$\mathrm{Conj}(P) = \{gPg^{-1} \mid g \in G\}.$$

G の p 部分群 H に対し, $H \subseteq P'$ となる $P' \in \mathrm{Conj}(P)$ の個数を $n_P(H)$ とおく. このとき, G の任意の p 部分群 H に対して,

$$n_P(H) \equiv |\mathrm{Conj}(P)| \equiv 1 \pmod p$$

が成り立つ[5].

［証明］ H を G の p 部分群とする. H の $\mathrm{Conj}(P)$ への作用

$$H \times \mathrm{Conj}(P) \to \mathrm{Conj}(P), \quad (h, P') \mapsto h \circ P' = hP'h^{-1}$$

を考える. 各 $P' \in \mathrm{Conj}(P)$ に対し, 上の作用による P の軌道を $\mathrm{Orb}_H(P')$ と書く:

$$\mathrm{Orb}_H(P') = \{h \circ P' \mid h \in H\}.$$

[5] $n_P(H)$ が H に依存するのに対して $\mathrm{Conj}(P)$ が H には無関係であることが重要である.

$\mathrm{Conj}(P)$ に属する 2 つの Sylow p 部分群が互いに共役であるという関係は, $\mathrm{Conj}(P)$ 上の同値関係である. 各々の $\mathrm{Orb}_H(P')$ は, その同値関係による同値類にほかならない. $\mathcal{U}$ を完全代表系とする. このとき,

$$\mathrm{Conj}(P) = \bigcup_{P' \in \mathcal{U}} \mathrm{Orb}_H(P') \quad (\text{集合の直和})$$

が成り立つ. したがって,

$$|\mathrm{Conj}(P)| = \sum_{P' \in \mathcal{U}} |\mathrm{Orb}_H(P')|.$$

また, 各 $P' \in \mathrm{Conj}(P)$ に対し, P' の固定群を $\mathrm{Stab}_H(P')$ と書く:

$$\mathrm{Stab}_H(P') = \{h \in H \mid h \circ P' = P'\}.$$

すると,

$$|\mathrm{Orb}_H(P')| = \frac{|H|}{|\mathrm{Stab}_H(P')|}.$$

特に, $|\mathrm{Orb}_H(P')|$ は $|H|$ の約数である. $|H|$ は p の冪だから, $|\mathrm{Orb}_H(P')|$ もまた p の冪である. よって, $|\mathrm{Orb}_H(P')| = 1$ または $|\mathrm{Orb}_H(P')| \equiv 0 \pmod{p}$. 補題 3.5 より,

$$\begin{aligned}
|\mathrm{Orb}_H(P')| = 1 &\iff hP'h^{-1} = P' \ (\forall h \in H) \\
&\iff H \subseteq N_G(P') \\
&\iff H \subseteq P'.
\end{aligned}$$

また, 完全代表系 $\mathcal{U}$ をどのように選んでも, 同値類が 1 元集合のとき, その元は必ず $\mathcal{U}$ に含まれる. すなわち,

$$\begin{aligned}
|\mathrm{Orb}_H(P')| = 1 &\Longrightarrow \mathrm{Orb}_H(P') = \{P'\} \\
&\Longrightarrow P' \in \mathcal{U}.
\end{aligned}$$

ゆえに,

$$\begin{aligned}
n_P(H) &= \#\{P' \in \mathrm{Conj}(P) \mid H \subseteq P'\} \\
&= \#\{P' \in \mathrm{Conj}(P) \mid |\mathrm{Orb}_H(P')| = 1\} \\
&= \#\{P' \in \mathcal{U} \mid |\mathrm{Orb}_H(P')| = 1\}.
\end{aligned}$$

したがって,

$$\begin{aligned}
|\mathrm{Conj}(P)| &= \sum_{\substack{P' \in \mathcal{U} \\ |\mathrm{Orb}_H(P')| = 1}} |\mathrm{Orb}_H(P')| + \sum_{\substack{P' \in \mathcal{U} \\ |\mathrm{Orb}_H(P')| > 1}} |\mathrm{Orb}_H(P')| \\
&= \sum_{\substack{P' \in \mathcal{U} \\ |\mathrm{Orb}_H(P')| = 1}} 1 + \sum_{\substack{P' \in \mathcal{U} \\ |\mathrm{Orb}_H(P')| > 1}} |\mathrm{Orb}_H(P')| \\
&\equiv n_P(H) \pmod{p}.
\end{aligned}$$

いま, H として特に P を考える．$P \in \mathrm{Conj}(P)$ かつ $P \subseteq P$ である．また, 任意の $P' \in \mathrm{Conj}(P)$ に対して, $P \subseteq P'$ ならば, P が Sylow p 部分群であることから $P = P'$. よって, $n_P(P) = 1$. ゆえに,

$$|\mathrm{Conj}(P)| \equiv n_P(P) = 1 \pmod p.$$

$\mathrm{Conj}(P)$ は H に無関係であるから, G の任意の p 部分群 H に対して,

$$n_P(H) \equiv |\mathrm{Conj}(P)| \equiv 1 \pmod p$$

が成り立つ． □

［定理 3.7（Sylow の定理）］ G を有限群, p を素数とする．P を Sylow p 部分群とし, H を G の p 部分群とする．このとき, P の G における共役部分群で H を含むものが存在する．

［証明］ 補題 3.6 より, 特に $n_P(H) \neq 0$ である．すなわち, P の G における共役部分群で H を含むものが存在する． □

［系 3.8］ G を有限群, p を素数とする．このとき, G の p 部分群のうちで包含関係について極大なものは G の Sylow p 部分群である．

［証明］ H を G の p 部分群のうちで包含関係について極大なものする．定理 3.1 より, G の Sylow p 部分群 G が存在する．定理 3.7 より, P の G における共役部分群 P' で H を含むものが存在する．P' もまた G の Sylow p 部分群である．H の極大性により, $P' = H$ となる． □

［定理 3.9（Sylow の定理）］ G を有限群, p を素数とする．このとき, G の Sylow p 部分群はすべて互いに共役である．

［証明］ G の 2 つの Sylow p 部分群 P, P' を任意にとる．定理 3.7 において H として P' を考えると, P の G における共役部分群 P'' で P' を含むものが存在することがいえる．P', P'' はともに G の Sylow p 部分群だから, $P' = P''$. したがって, P' は, P の G における共役部分群である． □

［系 3.10］ G を有限群, p を素数, P を G の Sylow p 部分群とする．このとき, P が G の正規部分群であるための必要十分条件は, G のすべての Sylow p 部分群が P に一致することである．したがって, G の Sylow p 部分群が一意的に存在するならば, その Sylow p 部分群は正規部分群である．

［**証明**］定理 3.7 より, G のすべての Sylow p 部分群は P の共役部分群である．したがって,

$$\begin{aligned}&P \text{ が } G \text{ の正規部分群}\\ \Longleftrightarrow\ &G \text{ における } P \text{ の共役部分群はすべて } P \text{ に一致する}\\ \Longleftrightarrow\ &G \text{ のすべての Sylow } p \text{ 部分群が } P \text{ に一致する}\end{aligned}$$

が成り立つ. □

［**系 3.11**］G を有限群, p を素数とする．G の Sylow p 部分群の全体からなる集合を $\mathrm{Syl}(p)$ とおく．このとき, G の $\mathrm{Syl}(p)$ への作用

$$G \times \mathrm{Syl}(p) \to \mathrm{Syl}(p), \quad (g,\, P) \mapsto g \circ P = gPg^{-1}$$

は推移的である.

［**証明**］定理 3.9 より, 任意の $P,\, P' \in \mathrm{Syl}(p)$ に対して, ある $g \in G$ が存在して $P' = g \circ P$ が成り立つ．よって, 作用は推移的である. □

［**系 3.12**］G を有限群, p を素数とする．G の Sylow p 部分群の全体からなる集合を $\mathrm{Syl}(p)$ とおく．また, P を G の Sylow p 部分群とし, P の G における共役部分群の全体からなる集合を $\mathrm{Conj}(P)$ とおく．このとき, $\mathrm{Conj}(P) = \mathrm{Syl}(p)$ が成り立つ.

［**証明**］$P' \in \mathrm{Syl}(p)$ を任意にとる．すると, 定理 3.9 より P と P' は互いに共役である．よって, $P' \in \mathrm{Conj}(P)$．ゆえに, $\mathrm{Syl}(p) \subseteq \mathrm{Conj}(P)$．逆の包含関係は明らか. □

［**定理 3.13（Sylow の定理）**］G を有限群, p を素数とする．また, G の Sylow p 部分群の個数を n_p とおく．このとき, $n_p \equiv 1 \pmod p$ が成り立つ．また, n_p は $|G|$ の約数である.

［**証明**］定理 3.1 より, G の Sylow p 部分群 P が存在する．系 3.12 より, $n_p = |\mathrm{Conj}(P)|$．補題 3.6 より, $|\mathrm{Conj}(P)| \equiv 1 \pmod p$．また, 系 1.2 より, $|\mathrm{Conj}(P)| = (G : N_G(P))$．これは $|G|$ の約数である. □

［**例 3.14**］G を有限群, p を素数とし, G の位数は p の冪であるとする．このとき, G の Sylow p 部分群は G 自身である.

［例 3.15］ G を有限 Abel 群, p を素数とする．Abel 群の部分群はすべて正規部分群なので, G の Sylow p 部分群は一意的に存在する．そして,

$$G(p) = \{x \in G \mid \text{ある整数 } n \geq 0 \text{ が存在して } p^n x = 0\}$$

が G のただ 1 つの Sylow p 部分群である．有限 Abel 群の基本定理によって, G は

$$G \cong \bigoplus_{i=1}^{s} \left(\bigoplus_{j=1}^{t_i} \mathbb{Z}/p_i^{e_{ij}}\mathbb{Z} \right)$$

と直和分解される．ただし, p_1, p_2, ..., p_s は相異なる素数である．このとき,

$$G(p_i) \cong \bigoplus_{j=1}^{t_i} \mathbb{Z}/p_i^{e_{ij}}\mathbb{Z}$$

となる.

参考文献

[1] 足立恒雄: ガロア理論講義, 日本評論社, 1996.

[2] J. J. Rotman: An Introduction to the Theory of Groups, 4th ed., Springer-Verlag, 1995.