シロー部分群

澤野嘉宏　学習院大学

Abstract. 有限群 G の構造について考える．有限群 G が可換であるなら，

$$G \simeq \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_r),\ a_1, a_2, \cdots, a_r \geq 2$$

なる同型が存在するのは既知の事実として認める．これは有限生成 PID 加群の構造定理を $\mathbb{Z}$ に対して適用しただけだからである．ここでは，非可換群の構造を考察する．

1. 中心化群，正規化群，類方程式

定義 1.1. $M \subset G$ に対して，

$$Z(M) = \{g \in G : \text{すべての } m \in M \text{ に対して } gm = mg\} : M \text{ の中心化群} \tag{1.1}$$

$$N(M) = \{g \in G : gM = Mg\} : M \text{ の正規化群} \tag{1.2}$$

と定める．ここで，$Z(G)$ を G の中心という．

補題 1.2. $Z(G)$ は正規部分群である．

証明. $a \in Z(G), b \in G$ に対して，$b^{-1}ab \in Z(G)$ つまり

$$b^{-1}abc = cb^{-1}ab,\ c \in G$$

を示そう．実際，$a \in Z(G)$ を用いて計算すると，

$$b^{-1}abc = b^{-1}a(bc) = b^{-1}bca = ca,\ cb^{-1}ab = cb^{-1}ba = ca$$

である．■

定義 1.3. $x, y \in G$ に対して，$x = h^{-1}yh$ なる $h \in G$ が存在するとき，x, y は共役であるという．

補題 1.4. $x \in Z(G)$ のとき，x と共役な G の元は x のみである．

証明. $h, y \in G$ に対して，$x = h^{-1}yh$ という関係があったとする．$x = h^{-1}xh$ であるから，連立して

$$h^{-1}yh = h^{-1}xh$$

より，$x = y$ が得られる．■

これから，類等式というものを導出する．

次の方法で，G を分割する．

0-a $G = Z(G)$ のときは，$G = Z(G)$ を 1 つの集まりからなる分割とする．
0-b $G \supsetneq Z(G)$ のときは，$a_1 \in G \setminus Z(G)$ を任意に取ってくる．

a_1 と共役なもの全体を A_1 と書く．

1-a $G = Z(G) \cup A_1$ のときは，この和集合を以ってして，G の分割とする．
1-b $G \supsetneq (Z(G) \cup A_1)$ のときは，$a_2 \in G \setminus (Z(G) \cup A_1)$ を任意に取ってくる．

a_2 と共役なもの全体を A_2 と書く.

2-a $G = Z(G) \cup (A_1 \cup A_2)$ のときは，この和集合を以ってして，G の分割とする.
2-b $G \supsetneq (Z(G) \cup (A_1 \cup A_2))$ のときは，$a_3 \in G \setminus (Z(G) \cup (A_1 \cup A_2))$ を任意に取ってくる.

以下，この操作を繰り返していく．G の数が有限なので，N 回目の段階では $N-a$ に入る．このとき，得られた $a_1, a_2, \cdots, a_N$ につき次のことが成り立つ.

補題 1.5. $g \in Z(G)$ でないならば，$g = h^{-1}a_k h$ となる $k = 1, 2, \cdots, N$ と $h \in G$ が成り立つ.

a_k の正規化群を N_{a_k} と表す．このとき，つぎのことが成り立つ.

補題 1.6. $g^{-1}a_k g = h^{-1}a_k h$ である必要十分条件は $hg^{-1} \in N_{a_k}$ である．したがって，a_k と共役であるような $g \in G$ の個数は $\sharp(G : N_{a_k}) = \sharp G / \sharp N_{a_k}$ である.

以上のことから，次の定理が成り立つ.

定理 1.7 (類方程式)**.** 有限群 G が与えられたとする．次の条件を満たしている $A \subset G \setminus Z(G)$ が存在して，

$$\sharp G = \sharp Z(G) + \sum_{a \in A} \sharp(G/N(\{a\}))$$

が成り立つ.

> [条件] $g \in G \setminus Z(G)$ に対して，$a \in A$ が一意的に存在して，$g = h^{-1}ah$ なる $h \in G$ による表示が可能である.

2. シロー部分群

素数 p は通常固定して，0 以上の整数 $q = q(G)$, $r = r(G)$ を q は p とは互いに素で $\sharp G = p^r q$ となるように取っておく.

$\sharp H = p^r$ となる部分群 H が存在することを示したい.

定義 2.1. $\sharp H = p^r$ となる部分群 H のことを G の p-シロー部分群という.

次のコセット分解を用いた補題が考察の鍵になる.

補題 2.2. K, H を G の部分群とする.

$$\sharp\{k^{-1}Hk : k \in K\} = \sharp K / \sharp(K \cap N(H))$$

が成り立つ.

証明. $k_1, k_2 \in K$ につき，${k_1}^{-1}Hk_1 = {k_2}^{-1}Hk_2$ である必要十分条件は $k_2{k_1}^{-1} \in N(H)$ である．ここで，$K = \displaystyle\coprod_{a \in S}(K \cap N(H))a$ をコセット分解とすると，$a_1, a_2 \in S$ が異なるなら，$a_1a_2^{-1} \notin K \cap N(H)$ となる．したがって，

$$\begin{aligned}
\sharp\{k^{-1}Hk : k \in K\} &= \sharp\{(ka)^{-1}H(ka) : k \in K \cap N(H),\, a \in S\} \\
&= \sharp\{a^{-1}k^{-1}Hka : k \in K \cap N(H),\, a \in S\} \\
&= \sharp\{a^{-1}Ha : k \in K \cap N(H),\, a \in S\} \\
&= \sharp S \\
&= \sharp K / \sharp(K \cap N(H))
\end{aligned}$$

∎

定理 2.3. p-シロー部分群は少なくともひとつ存在する．

証明. $\sharp G$ に関する帰納法で証明する．$\sharp G = 1$ のときは G が自明な群であるから明らかである．p が $\sharp Z(G)$ を割るときは，アブストラクトに書いたことより明らかである．p が $\sharp Z(G)$ を割らないときは類方程式

$$\sharp G = \sharp Z(G) + \sum_{a \in A} \sharp(G/N(\{a\}))$$

より，

$$0 \equiv \sharp Z(G) + \sum_{a \in A} \sharp(G/N(\{a\})) \bmod p$$

となるので，$a \in A \subset G$ で $\sharp(G/N(\{a\}))$ が p の倍数でないものが存在する．このとき，$A \cap Z(G) \neq \emptyset$ であるから，$N(\{a\}) \subsetneq G$ である．$r(\{N(\{a\})\}) = r(G)$ に注意する．実際に，$\sharp(G/N(\{a\}))$ が p の倍数でないからである．$N(\{a\})$ は G より位数が真に小さいので，$H \subset N(\{a\})$ となる部分群で，$\sharp H = p^{r(N(\{a\}))} = p^{r(G)}$ である．$H \subset N(\{a\}) \subset G$ であるから，この G が求めるものである．∎

定理 2.4. p-シロー部分群は互いに共役である．

証明. H, K をそれぞれ p-シロー部分群とする．p-シロー部分群の集まり $\mathcal{A}$ を

$$\mathcal{A} = \{L : g \in G \text{ を用いて } L = g^{-1}Hg \text{ と表される }\}$$

で定める．$\mathcal{A} \ni K$ を示すのが目的である．

ここで，補題 2.2 より，$\sharp\mathcal{A}$ は $\sharp G/\sharp H$ 個の部分群からなる集合である．

$L_1, L_2 \in \mathcal{A}$ は $L_1 = g^{-1}L_2g,\ g \in K$ なる関係があるとき，同値であるということにして，$\mathcal{A}$ を同値類で分ける．すると，$L \in \mathcal{A}$ のとき，i が一意的に存在して，$k \in K$ を用いて $L = k^{-1}L_ik$ となるという性質を持つ $L_1, L_2, \cdots, L_s$ が得られる．

補題 2.2 より，

$$\sharp\{k^{-1}L_ik : k \in K\} = \sharp K/\sharp K \cap N(L_i)$$

となり，

[条件 1] $\{k^{-1}L_ik : k \in K\}$ は p の冪であることがわかる．

対象性を考慮して，$\sharp\{k^{-1}L_ik : k \in K\}$ は i について増加しているとする．また，この条件を用いて $\mathcal{A}$ を分割してみると，

$$\sharp\mathcal{A} = \sum_{i=1}^{s} \sharp\{k^{-1}L_ik : k \in K\}$$

が得られる．$\sharp A = \sharp G/\sharp H$ は p では割り切れない．$\sharp\{k^{-1}L_ik : k \in K\}$ は i について増加しているとしているので，p は $\sharp\{k^{-1}L_1k : k \in K\}$ の約数ではない．条件 1 も考慮して，

$$\sharp\{k^{-1}L_1k : k \in K\} = \sharp K/\sharp K \cap N(L_i) = 1$$

である．すなわち，$K = N(L_1)$ である．$N(L_1) \supset L_1$ で，$\sharp L_1 = \sharp K = p^r$ だから，$K = L_1 \in \mathcal{A}$ である．∎

定理 2.5. G の p-シロー部分群の個数を N 個とすると，

$$N | \sharp G,\ p | N-1$$

が成り立つ．

証明. 初めの式は補題 2.2 より，

$$N = \sharp\{g^{-1}Hg \,:\, g \in G\} = \sharp G/\sharp(G \cap N(H))|\sharp G$$

より明らかである．２番目の式は，定理 2.4 の証明中の記号を用いて

$$N = \mathcal{A} = 1 + \sum_{i=2}^{s} \sharp K/\sharp(K \cap N(L_i))$$

である．$i \geq 2$ につき，$K = K \cap N(L_i)$ が成り立つと個数に関する考察から，$K = L_i$ となり矛盾である．したがって，$p|\sharp K/\sharp(K \cap N(L_i))$ となる．

$$p|\sum_{i=2}^{s} \sharp G/\sharp(G \cap N(L_i)) = N - 1$$

より明らかである．■

3. 問題例

問題 3.1. 77 個の元からなる群は可換である．

証明. $\sharp G = 77$ であるような群 G を取ってくる．N を 7-シロー部分群の個数とすると，

$$N|77,\, 7|N-1$$

である．最初の条件より，$N = 1, 7, 11, 77$ であるが，２番目の条件にかなうのは $N = 1$ しかない．同様に，M を 11-シロー部分群の個数は 1 つとわかる．それぞれ G_7, G_{11} で 1 つしかない $7, 11$-シロー部分群とするとき，$G_7 \cap G_{11} = \{e_G\}$ であるから，

$$\sharp(G \setminus (G_7 \cap G_{11})) = 77 - 7 - 11 + 1 = 60$$

である．この 60 個からなる集合は位数が 77 の集合である．60 個の元のうち任意に g をひとつ取ってくると，g^{77} で初めて e に戻る．つまり，

$$\mathbb{Z} \to G,\, n \mapsto g^n$$

の核は $77\mathbb{Z}$ ということであるから，$\mathbb{Z}/77\mathbb{Z} \simeq G$ となり，すでに知られている $\mathbb{Z}/77\mathbb{Z}$ 以外に G の構造はありえないということなりなる．■

問題 3.2. p^2 個からなる群 G は可換である．

証明. G が巡回群であるなら，何も示すことはないので，G は巡回群ではないとする．類方程式より

$$|G| = Z(G) + \sum_{a \in A} \sharp G/\sharp N(a),\, \sharp G > \sharp N(a) > 1$$

が成り立つ．

$$p|\sum_{a \in A} \sharp G/\sharp N(a)$$

であるから，$\sharp Z(G) \geq p$ となる．すると，$Z(G), G/Z(G)$ は巡回群である．このことから，$a \in Z(G)$ と $b \in G \setminus Z(G)$ が存在して，$g \in G$ に対して，$g = b^l\, a^m$ なる表示が可能である．ところが，$a \in Z(G)$ なので，この表示から G が巡回群になる．■