小さい位数の群の分類

MATHEMATICS.PDF

2013-08-19

目 次

1　生成元と基本関係によって定義される群について

整数 $n \geq 1$ に対して, 1 つの生成元 a と基本関係 $a^n = e$ によって定義される群は位数 n の巡回群 (cyclic group) である. これを C_n で表す.

整数 $n \geq 3$ に対して, 2 つの生成元 a, b と基本関係

$$a^n = b^2 = e, \quad ba = a^{n-1}b$$

によって定義される群は位数 $2n$ の非 Abel 群である. これを位数 $2n$ の二面体群 (dihedral group) といい, D_{2n} で表す.

整数 $n \geq 2$ に対して, 2 つの生成元 a, b と基本関係

$$a^{2n} = e, \quad a^n = b^2, \quad ba = a^{2n-1}b$$

によって定義される群は位数 $4n$ の非 Abel 群である. これを位数 $4n$ の四元数群 (quaternion group) といい, Q_{4n} で表す.

群 G は生成元 a_1, a_2, ..., a_n と基本関係

$$R_1(a_1, a_2, \ldots, a_n) = \cdots = R_m(a_1, a_2, \ldots, a_n) = e$$

によって定義されるものとし, 群 G' は b_1, b_2, ..., b_n によって生成され, それらの生成元は関係式

$$R_1(b_1, b_2, \ldots, b_n) = \cdots = R_m(b_1, b_2, \ldots, b_n) = e$$

を満たすものとする. このとき, 全射準同型写像 $\phi : G \to G'$ が存在して, 各 $i = 1, 2, \ldots, n$ に対して $\phi(a_i) = b_i$ を満たす. $|G| = |G'| < \infty$ のとき, ϕ が全射であることと単射であることは同値であるから, ϕ は同型写像である.

2　位数 1 の群

[定理 2.1] 位数 1 の群は単位群である.

[証明] G を位数 1 の群とする. G は単位元 e を必ずもつから, $\{e\} \subseteq G$ である. G の位数 $|G|$ は 1 であるから, $|\{e\}| = |G|$. ゆえに, $G = \{e\}$. □

3　位数 p の群

[定理 3.1] 素数位数の群は巡回群である.

[証明] p を素数とし, G を位数 p の群とする. a を G の単位元 e 以外の元とし, a の位数を l とおく. すなわち, l は a によって生成される G の部分群 $\langle a \rangle$ の位数である. l は G の位数 p の約数である. p は素数であり, p の正の約数は 1 と p しかないから, $l = 1$ または p である. $a \neq e$ であるから, $l = p$. よって, $\langle a \rangle \subseteq G$ かつ $|\langle a \rangle| = |G|$. ゆえに, $G = \langle a \rangle$. すなわち, G は a によって生成される巡回群である. □

4　位数 p^2 の群

［補題 4.1］ G を群, p を素数, $k \geq 1$ を整数とし, $|G| = p^k$ であるとする. また, $Z(G)$ を G の中心とする. このとき, $|Z(G)|$ は p の倍数である.

［証明］ C_1, C_2, …, C_s を 2 つ以上の元を含むすべての G の共役類とすると, 類等式

$$|G| = |Z(G)| + \sum_{i=1}^{s} |C_i|,$$
$$(G : N_G(x_i)) = |C_i| > 1, \quad x_i \in C_i$$

が成り立つ. ただし, $N_G(x_i)$ は x_i の正規化群である. $|G|$ は p の倍数である. また, 各 $(G : N_G(x_i))$ は, $|G| = p^k$ の 1 より大きい約数だから, p の倍数である. ゆえに, $|Z(G)|$ は p の倍数である. □

［補題 4.2］ 位数が p^2 の群は Abel 群である.

［証明］ $G = Z(G)$ をいえばよい. $|Z(G)|$ は $|G|$ の約数であるが, 補題 4.1 より $|Z(G)| = p$ または p^2 である. いま, $|Z(G)| = p$ と仮定して矛盾を導く. $Z(G)$ は G の正規部分群だから, 剰余群 $G/Z(G)$ が定まる. $G/Z(G)$ の位数を計算すると,

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = p.$$

素数位数の群は巡回群だから, $G/Z(G)$ は巡回群であり, ある $a \in G$ が存在して,

$$G/Z(G) = \langle aZ(G) \rangle = \{a^i Z(G) \mid i = 0, 1, \ldots, p-1\}.$$

よって,

$$G = \bigcup_{i=0}^{p-1} a^i Z(G).$$

ゆえに, G のすべての元は

$$a^i z, \quad z \in Z(G)$$

の形で表される. ところが,

$$a(a^i z) = a^{i+1} z = (a^i z) a$$

より, $a \in Z(G)$. さらに,

$$\begin{aligned} a \in Z(G) &\Longrightarrow aZ(G) = Z(G) \\ &\Longrightarrow G/Z(G) = \{Z(G)\} \\ &\Longrightarrow |G/Z(G)| = 1. \end{aligned}$$

これは $|G/Z(G)| = p$ と矛盾する. したがって, $|Z(G)| = p^2$ でなければならない. すると, $Z(G) \subseteq G$ かつ $|Z(G)| = |G|$ となり, $G = Z(G)$ がいえる. □

［**補題 4.3**］p を素数とする．G を位数 p^2 の群，A, B を G の位数 p の部分群とし，$A \neq B$ であるとする．このとき，$A \cap B = \{e\}$ かつ $G = AB$ が成り立つ．

［**証明**］$A \cap B$ は A の部分群であるから，$|A \cap B|$ は $|A| = p$ の約数である．p は素数だから，$|A \cap B| = 1$ または p である．もし仮に $|A \cap B| = p$ であるとすると，$A \cap B \subseteq A$ かつ $|A \cap B| = |A|$ より $A \cap B = A$. よって，$A \subseteq B$. これと $|A| = |B|$ より $A = B$ を得る．ところが，これは $A \neq B$ であるという仮定に反する．よって，$|A \cap B| = 1$. ゆえに，$A \cap B = \{e\}$. さらに，

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|} = p^2 = |G|.$$

これと $AB \subseteq G$ より，$G = AB$ がいえる． □

［**定理 4.4**］p を素数とする．このとき，位数 p^2 の群は，C_{p^2} または $C_p \times C_p$ に同型である．

［**証明**］G を位数 p^2 の群とする．G の元の位数は，G の位数の約数であるから，1, p, p^2 のいずれかである．もし位数 p^2 の元が存在すれば，G は巡回群になる．以下，G は位数 p^2 の元をもたないと仮定し，そのとき $G \cong C_p \times C_p$ が成り立つことを示す．

単位元は位数 1 の元であり，逆に位数 1 の元は単位元のみである．よって，G の単位元以外の元の位数は p である．そこで，G の単位元以外の元 a をとり，a によって生成される G の部分群を A とする．また，A に属さない G の元 b をとり，b によって生成される G の部分群を B とする．a, b の位数はともに p なので，$|A| = |B| = p$ である．補題 4.3 より，$A \cap B = \{e\}$ かつ $G = AB$ である．さらに，補題 4.2 より G は Abel 群であるから，A, B はともに G の正規部分群である．ゆえに，G は A, B の直積である．したがって，

$$G \cong A \times B \cong C_p \times C_p$$

が成り立つ． □

［**注意 4.5**］巡回群 C_{p^2} と群の直積 $C_p \times C_p$ は同型ではない．なぜなら，C_{p^2} は位数 p^2 の元をもつが，$C_p \times C_p$ は位数 p^2 の元をもたないからである．実際，すべての $x \in C_p \times C_p$ に対して，$x^p = e$ が成り立つ．

5　位数 pq の群

［**補題 5.1**］G を群，A, B を G の部分群とし，

$$|G| = |A| \cdot |B|, \quad \gcd(|A|, |B|) = 1$$

であるとする．このとき，

$$G = AB, \quad A \cap B = \{e\}$$

が成り立つ．

［**証明**］$x \in A \cap B$ とする．$x \in A$ より x の位数は $|A|$ の約数であり，$x \in B$ より x の位数は $|B|$ の約数である．よって，x の位数は $|A|$ と $|B|$ の公約数であるが，$\gcd(|A|, |B|) = 1$ であるから，x の位数は 1 である．よって，$x = e$．ゆえに，$A \cap B \subseteq \{e\}$．逆の包含関係は明らかであるから，$A \cap B = \{e\}$．さらに，

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|} = |G|.$$

これと $AB \subseteq G$ より，$G = AB$ を得る． □

［**定理 5.2**］p, q を素数とし，$p > q$ かつ $p \not\equiv 1 \pmod{q}$ であるとする．このとき，位数 pq の群は巡回群である．

［**証明**］G を位数 pq の群とする．

Sylow の定理より，G の Sylow p 部分群の個数 k_p は，$|G| = pq$ の約数かつ $k_p \equiv 1 \pmod{p}$ を満たす．前者の条件より k_p は 1, q, p, pq のいずれかである．後者の条件と $p > q$ より，$k_p = 1$．よって，G の Sylow p 部分群は，ただ 1 つ存在し，G の正規部分群である．それを A とおく．$|A| = p$ である．A は素数位数なので巡回群である．

再び Sylow の定理より，G の Sylow q 部分群の個数 k_q は，$|G| = pq$ の約数かつ $k_q \equiv 1 \pmod{q}$ を満たす．前者の条件より k_q は 1, q, p, pq のいずれかである．後者の条件と $p \not\equiv 1 \pmod{q}$ より，$k_q = 1$．よって，G の Sylow q 部分群は，ただ 1 つ存在し，G の正規部分群である．それを B とおく．$|B| = q$ である．B は素数位数なので巡回群である．

さて，

$$|G| = |A| \cdot |B|, \quad \gcd(|A|, |B|) = 1$$

であるから，補題 5.1 より，

$$G = AB, \quad A \cap B = \{e\}$$

が成り立つ．A, B は G の正規部分群だったから，G は A, B の直積である．したがって，

$$G \cong A \times B \cong C_p \times C_q \cong C_{pq}$$

が成り立つ． □

［**例 5.3**］位数 15 の群は巡回群である．

［**補題 5.4**］G を群，A, B を G の巡回部分群，a, b をそれぞれ A, B の生成元とする．また，AB が G の部分群であるとする．このとき，$AB = \langle a, b \rangle$ が成り立つ．

［**証明**］$A = \langle a \rangle$, $B = \langle b \rangle$ より，

$$\begin{aligned} AB &= \{xy \mid x \in A, y \in B\} \\ &= \{a^i b^j \mid i, j \in \mathbb{Z}\} \\ &\subseteq \langle a, b \rangle. \end{aligned}$$

逆に，$a = ae \in AB$, $b = eb \in AB$ であり，AB は G の部分群であるから，$\langle a, b \rangle \subseteq AB$．ゆえに，$AB = \langle a, b \rangle$． □

［**補題 5.5**］G を群, a, b を G の元, i を整数とし,

$$bab^{-1} = a^i$$

が成り立つとする. このとき, 任意の整数 $n \geq 1$ に対して,

$$b^n ab^{-n} = a^{i^n}$$

が成り立つ.

［**証明**］n に関する数学的帰納法により証明する. $n = 1$ のときは明らかである. $n - 1$ に対して正しいと仮定すると,

$$\begin{aligned} b^n ab^{-n} &= b(b^{n-1}ab^{-(n-1)})b^{-1} = ba^{i^{n-1}}b^{-1} \\ &= (bab^{-1})^{i^{n-1}} = (a^i)^{i^{n-1}} \\ &= a^{i^n}. \end{aligned}$$

ゆえに, n のときも正しい. したがって, すべての n に対して成り立つ. □

［**定理 5.6**］p, q を素数とし, $p > q$ かつ $p \equiv 1 \pmod{q}$ であるとする. また, i_0 を合同方程式 $x^q \equiv 1 \pmod{p}$ の整数解で $2 \leq i_0 \leq p - 1$ を満たすものとする. このとき, 位数 pq の群は, C_{pq} (巡回群) に同型であるか, または 2 つの生成元 a, b と基本関係

$$a^p = b^q = e, \quad bab^{-1} = a^{i_0}$$

によって定義される非 Abel 群[1)]に同型である.

［**証明**］G を位数 pq の群とする.

Sylow の定理より, G の Sylow p 部分群の個数 k_p は, $|G| = pq$ の約数かつ $k_p \equiv 1 \pmod{p}$ を満たす. 前者の条件より k_p は 1, q, p, pq のいずれかである. 後者の条件と $p > q$ より, $k_p = 1$. よって, G の Sylow p 部分群は, ただ 1 つ存在し, G の正規部分群である. それを A とおく. $|A| = p$ である. A は素数位数なので巡回群である. A の生成元を a とおく.

再び Sylow の定理より, G の Sylow q 部分群 B が存在する. $|B| = q$ である. B は素数位数なので巡回群である. B の生成元を b とおく.

さて,

$$|G| = |A| \cdot |B|, \quad \gcd(|A|, |B|) = 1$$

であるから, 補題 5.1 より,

$$G = AB, \quad A \cap B = \{e\}$$

が成り立つ. A, B は G の巡回部分群であるから, 補題 5.4 より G は a, b によって生成される. A は G の正規部分群だから, $bab^{-1} \in A$. ゆえに, ある整数 i が存在して,

$$bab^{-1} = a^i, \quad 0 \leq i \leq p - 1$$

[1)] 後者の群が非可換であることは, 条件 $bab^{-1} = a^{i_0}$ より $ab \neq ba$ となることからわかる.

と書ける. $b^q = e$ であることと補題 5.5 より,

$$a = b^q a b^{-q} = a^{i^q}.$$

よって,

$$a^{i^q - 1} = e.$$

a の位数が p であることから, $i^q \equiv 1 \pmod{p}$. この i に関する合同方程式は p を法として q 個の整数解をもつ. $i = 1$ 以外の整数解を i_0 とすると, $1, i_0, i_0^2, \ldots, i_0^{p-1}$ が法 p で異なる整数解のすべてである.

$i = 1$ のとき, $ba = ab$ であるが, G は a, b によって生成されるから, G が可換である. Abel 群の部分群は正規部分群であるから, B もまた G の正規部分群である. よって, G は A, B の直積である. したがって,

$$G \cong A \times B \cong C_p \times C_q \cong C_{pq}.$$

ここで, 最後の同型において $\gcd(p, q) = 1$ であることを用いた.

$i \neq 1$ のとき, ある整数 s $(1 \leq s \leq q-1)$ が存在して, G の生成元 a, b は関係式

$$a^p = b^q = e, \quad bab^{-1} = a^{i_0^s}$$

を満たす. また, ある整数 t が存在して, $st \equiv 1 \pmod{q}$ かつ $1 \leq t \leq q-1$ を満たす. 補題 5.5 より,

$$b^t a b^{-t} = a^{i_0^{st}} = a^{i_0}.$$

B は素数位数の巡回群であり, $b^t \neq e$ であるから, b^t もまた B の生成元である. b^t を改めて b と書くことにすれば, a, b は G の生成元であり, 関係式

$$a^p = b^q = e, \quad bab^{-1} = a^{i_0}$$

を満たす. □

[例 5.7] 位数 21 の群は, C_{21} に同型であるか, または 2 つの生成元 a, b と基本関係

$$a^p = b^q = e, \quad bab^{-1} = a^2$$

によって定義される非 Abel 群に同型である.

[系 5.8] p を奇素数とする. このとき, 位数 $2p$ の群は C_{2p} (巡回群) または D_{2p} (二面体群) に同型である.

[証明] $q = 2, i_0 = p - 1$ として定理 5.6 を適用すればよい. □

[例 5.9] 位数 6 の群は C_6 または D_6 に同型である. なお, D_6 は 3 次対称群 S_3 に同型である.

6　位数 8 の群

［**定理 6.1**］位数 8 の Abel 群は, C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$ のいずれかに同型である.

［**証明**］G を位数 8 の Abel 群とする. G の元の位数は, $|G| = 8$ の約数であるから, 1, 2, 4, 8 のいずれかである. また, 単位元は位数 1 の元であり, 逆に位数 1 の元は単位元のみである. よって, G の単位元以外の元の位数は 2, 4, 8 のいずれかである.

G が位数 8 の元をもつとき: G は巡回群になる. すなわち, $G \cong C_8$.

G が位数 8 の元をもたず, 位数 4 の元をもつとき: G の位数 4 の元を a とし, a によって生成される G の部分群を A とする. $|A| = 4$ であり, $(G : A) = |G|/|A| = 2$ である. さらに, A に属さない G の元 b をとる. b の位数は 2 または 4 である.

b の位数が 2 の場合. b によって生成される G の部分群を B とする. $b \notin A$ より, $A \cap B = \{e\}$. 再び $b \notin A$ より $Ab \neq A$ であり, かつ $(G : A) = 2$ であるから,

$$G = A \cup Ab \subseteq AB \subseteq G.$$

よって, $G = AB$ である. G は Abel 群であるから, A, B はともに G の正規部分群である. よって, G は A, B の直積である. したがって,

$$G \cong A \times B \cong C_4 \times C_2.$$

b の位数が 4 の場合. $(G : A) = 2$ であるから, $b^2A = (bA)^2 = A$. これより, $b^2 \in A$ を得る. a の位数は 4 であるから, ある整数 i が存在して,

$$b^2 = a^i, \quad 0 \leq i \leq 3$$

と書ける. $i = 0$ のときは b の位数が 4 であることに反する. $i = 1, 3$ のとき,

$$e = b^4 = a^{2i} = a^2$$

となって, a の位数が 4 であることに反する. よって, $b^2 = a^2$ である. さて, $b' = ab$ とおく. もし仮に $b' \in A$ ならば $b = a^{-1}b' \in A$ となり b の定め方に反するから, $b' \notin A$. 特に, $b' \neq e$ である. さらに, G が Abel 群であることから,

$$b'^2 = (ab)^2 = a^2b^2 = a^4 = e.$$

よって, b' の位数は 2 である. したがって, 議論は b の位数が 2 の場合に帰着する.

G の単位元以外の元の位数がすべて 2 のとき: G の異なる 2 つの元 a, b をとり, $A = \langle a \rangle$, $B = \langle b \rangle$ とおくと, $A \cap B = \{e\}$ である. よって,

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|} = 4$$

このとき, 位数を比較すれば, $G \neq AB$ がわかる. そこで, G の元 c で $c \notin AB$ なるものをとり, $C = \langle c \rangle$ とおくと, $AB \cap C = \{e\}$. よって,

$$|ABC| = \frac{|AB| \cdot |C|}{|AB \cap C|} = 8.$$

これと $ABC \subseteq G$ より, $G = ABC$ となる. G は Abel 群だから, A, B, C は G の正規部分群である. ゆえに, G は A, B, C の直積である. すなわち,

$$G \cong A \times B \times C \cong C_2 \times C_2 \times C_2$$

が成り立つ. □

［補題 6.2］ G を群とし, G のすべての元 x に対して $x^2 = e$ が成り立つとする. このとき, G は可換である.

［証明］ G の元 x, y を任意にとる. 仮定より

$$x^2 = y^2 = (xy)^2 = e$$

であるから,

$$x^{-1} = x, \quad y^{-1} = y, \quad (xy)^{-1} = xy.$$

ゆえに,

$$yx = y^{-1}x^{-1} = (xy)^{-1} = xy.$$

したがって, G は可換である. □

［補題 6.3］ G を群, H を G の部分群とし, $(G : H) = 2$ であるとする. このとき, H は G の正規部分群である.

［証明］ $x \in G$ を任意にとる. $xH = Hx$ であることをいえばよい.
$x \in H$ のとき, $xH = H = Hx$ である.
$x \notin H$ のとき, 左剰余類について, $xH \neq H$ であり, $(G : H) = 2$ であることから,

$$G = H \cup xH.$$

同様に, 右剰余類について,

$$G = H \cup Hx.$$

ゆえに,

$$H \cup xH = H \cup Hx.$$

さらに, 一般に異なる同値類は互いに交わらないから,

$$H \cap xH = H \cap Hx = \emptyset.$$

したがって, $xH = Hx$ がいえる. 実際, $y \in xH$ とすると, $y \in H \cup xH = H \cup Hx$, すなわち $y \in H$ または $y \in Hx$. もし仮に $y \in H$ であるとすると, $y \in H \cap xH = \emptyset$ となり矛盾が生じるから, $y \notin H$. よって, $y \in Hx$. ゆえに, $xH \subseteq Hx$. 逆の包含関係についても同様. □

［定理 6.4］ 位数 8 の非 Abel 群は D_8 (二面体群) または Q_8 (四元数群) に同型である.

［**証明**］G を位数 8 の非 Abel 群とする.

G の元の位数は, $|G| = 8$ の約数であるから, 1, 2, 4, 8 のいずれかであるが, もし仮に位数 8 の元が存在すれば, G は巡回群になり, 非可換であることに反する. また, 単位元は位数 1 の元であり, 逆に位数 1 の元は単位元のみである. よって, G の単位元以外の元の位数は 2 または 4 である.

G は位数 4 の元 a を必ず持つ. なぜなら, もし仮に G が位数 2 の元しか持たなければ, 補題 6.2 より G は可換になり, 矛盾が生じる. a によって生成される G の部分群を A とする. $|A| = 4$ であり, $(G : A) = |G|/|A| = 2$ である. さらに, A に属さない G の元 b をとる.

G は a, b によって生成される. すなわち, $G = \langle a, b\rangle$ が成り立つ. 実際, $b \notin A$ より $Ab \neq A$ であり, かつ $(G : A) = 2$ であるから, $G = A \cup Ab$ である. $x \in G$ とすると, $x \in A$ または $x \in Ab$. いずれにせよ $x \in \langle a, b\rangle$ である. よって, $G \subseteq \langle a, b\rangle$. 逆の包含関係は明らかである.

補題 6.3 より A は G の正規部分群であるから, $bab^{-1} \in A$ である. ゆえに, ある整数 i が存在して,

$$bab^{-1} = a^i, \quad 0 \leq i \leq 3$$

と書ける. $b^2 = e$ であることと補題 5.5 より,

$$a = b^2ab^{-2} = a^{i^2}.$$

よって,

$$a^{i^2-1} = e.$$

a の位数が 4 であることから, $i^2 \equiv 1 \pmod 4$. ゆえに, $i = 1$ または 3 である. ところが, 前者は $ba = ab$ と同値であり, G は a, b で生成されるから, G が可換になってしまい, G が非 Abel 群であることに反する. よって, $i = 3$, すなわち, $bab^{-1} = a^3$ でなければならない. これは $ba = a^3b$ と同値である.

$|G/A| = (G : A) = 2$ であるから,

$$b^2A = (bA)^2 = A.$$

これより, $b^2 \in A$ を得る. ゆえに, ある整数 i が存在して,

$$b^2 = a^i, \quad 0 \leq i \leq 3$$

と書ける. b の位数は 2 または 4 であるから, $b^4 = e$. よって,

$$e = b^4 = a^{2i}.$$

a の位数は 4 であるから, $2i$ は 4 の倍数. よって, i は 2 の倍数. ゆえに, $i = 0$ または 2 でなければならない.

$i = 0$, すなわち $b^2 = e$ の場合. G の生成元 a, b は, 関係式

$$a^4 = b^2 = e, \quad ba = a^3b$$

を満たす. したがって, G は位数 8 の二面体群に同型である.

$i = 2$, すなわち $b^2 = a^2$ の場合. G の生成元 a, b は, 関係式

$$a^4 = e, \quad a^2 = b^2, \quad ba = a^3b$$

を満たす. したがって, G は位数 8 の四元数群に同型である. □

［**注意 6.5**］D_8 と Q_8 は同型でない. 実際, Q_8 は位数 2 の元を 1 個しかもたないが, D_8 は位数 2 の元を 5 個もつ.

7　位数 12 の群

［**定理 7.1**］位数 12 の Abel 群は, C_{12} または $C_2 \times C_6$ に同型である.

［**証明**］G を位数 12 の Abel 群とする. Sylow の定理より, G の Sylow 2-部分群 H および Sylow 3 部分群 K が存在する. $|G| = 2^2 \cdot 3$ より, $|H| = 4$, $|K| = 3$ であり,

$$|G| = |H| \cdot |K|, \quad \gcd(|H|, |K|) = 1$$

であるから, 補題 5.1 より,

$$G = HK, \quad H \cap K = \{e\}$$

が成り立つ. G は Abel 群だから, H, K はともに G の正規部分群である. よって, G は H, K の直積である. すなわち,

$$G \cong H \times K.$$

H の位数は 4 だから, $H \cong C_4$ または $H \cong C_2 \times C_2$ である. また, K の位数は 3 だから, $K \cong C_3$ である. したがって, G が Abel 群のときは, 次の 2 通りの同型が考えられる.

$$G \cong C_4 \times C_3 \cong C_{12},$$
$$G \cong C_2 \times C_2 \times C_3 \cong C_2 \times C_6.$$

□

［**定理 7.2**］位数 12 の非 Abel 群は, D_{12} (二面体群), Q_{12} (四元数群), A_4 (4 次交代群) のいずれかに同型である.

［**証明**］G を位数 12 の非 Abel 群とする. G の Sylow 3 部分群の個数を k_3 とする. Sylow の定理より, $k_3 \equiv 1 \pmod 3$ であり, かつ k_3 は $|G| = 12$ の約数である. よって, $k_3 = 1$ または 4 である.

$k_3 = 1$ のとき: G の Sylow 3 部分群を K とおく. K は G の正規部分群である. $|G| = 2^2 \cdot 3$ なので, $|K| = 3$ である. K の位数は素数なので, K は巡回群である. K の生成元を s とすると, s の位数は 3 である. G の位数 3 の元が生成する部分群はすべて G の Sylow 3 部分群なので, K に一致する. よって, s, s^2 が G の位数 3 の元のすべてである. s の共役元の位数は s の位数に等しいから, s の共役元の個数は 2 以下である. 一方, s の正規化群 $N_G(s)$ を考えると, s の共役元の個数は $(G : N_G(s))$ に等しい. ゆえに, $(G : N_G(s)) = 1$ または 2. よって, $|N_G(s)| = 12$ または 6 となり, $N_G(s)$ の Sylow 2 部分群の中に位数 2 の元 t が存在して, $st = ts$ を満たす. このとき, st の位数は 6 である.

$a = st$ とおき, a によって生成される G の部分群を A とする. $|A| = 6$ であり, $(G : A) = |G|/|A| = 2$ である. さらに, A に属さない G の元 b をとり, b によって生成される G の部分群を B とする.

G は a, b によって生成される. すなわち, $G = \langle a, b \rangle$ が成り立つ. 実際, $b \notin A$ より $Ab \neq A$ であり, かつ $(G : A) = 2$ であるから, $G = A \cup Ab$ である. $x \in G$ とすると, $x \in A$ または $x \in Ab$. いずれにせよ $x \in \langle a, b \rangle$ である. よって, $G \subseteq \langle a, b \rangle$. 逆の包含関係は明らかである.

$(G:A)=2$ であるから, 補題 6.3 より A は G の正規部分群である. よって, $bab^{-1}\in A$ である. ゆえに, ある整数 i が存在して,

$$bab^{-1}=a^i,\quad 0\le i\le 5$$

と書ける. $b^2=e$ であることと補題 5.5 より,

$$a=b^2ab^{-2}=a^{i^2}.$$

よって,

$$a^{i^2-1}=e.$$

a の位数が 6 であることから, $i^2\equiv 1 \pmod 6$. ゆえに, $i=1$ または 5 である. ところが, 前者は $ba=ab$ と同値であり, G は a, b で生成されるから, G が可換になってしまい, G が非 Abel 群であることに反する. よって, $i=5$, すなわち, $bab^{-1}=a^5$ でなければならない. これは $ba=a^5b$ と同値である.

$|G/A|=(G:A)=2$ であるから,

$$b^2A=(bA)^2=A.$$

これより, $b^2\in A$ を得る. a の位数は 6 であるから, ある整数 i が存在して,

$$b^2=a^i,\quad 0\le i\le 5$$

と書ける. もし仮に $i=1$ または 5 ならば, b の位数は 12, したがって G は巡回群となって G が非可換であることに反する. もし仮に $i=2$ または 4 ならば, $b^4=a^2$ であるが, $ba=a^5b$ であったから,

$$a^4=a^{10}=(bab^{-1})^2=ba^2b^{-1}=b^4=a^2.$$

これより $a^2=e$ を得るが, a の位数が 6 であることに反する. よって, $i=0$ または 3 でなければならない.

$i=0$, すなわち $b^2=1$ の場合. G の生成元 a, b は, 関係式

$$a^6=b^2=e,\quad ba=a^5b$$

を満たす. したがって, G は位数 12 の二面体群に同型である.

$i=3$, すなわち $b^2=a^3$ の場合. G の生成元 a, b は, 関係式

$$a^6=e,\quad a^3=b^2,\quad ba=a^5b$$

を満たす. したがって, G は位数 12 の四元数群に同型である.

$k_3=4$ のとき: G の Sylow 3 部分群を K_1, K_2, K_3, K_4 とおく. G は共役により集合 $\Omega=\{K_1,K_2,K_3,K_4\}$ に作用する. すなわち,

$$G\times\Omega\to\Omega,\quad (g,K_i)\mapsto gK_ig^{-1}$$

は G の Ω への作用である. この作用による置換表現

$$\rho:G\to S_4,\quad g\mapsto\rho(g)$$

が, 各 $i=1,2,3,4$ に対して

$$K_{(\rho(g))(i)}=gK_ig^{-1}$$

とおくことによって定まる．ここで, S_4 は 4 次対称群である．各番号 i に対して, K_i の軌道を $\mathrm{Orb}(K_i)$ と書く．すなわち,

$$\mathrm{Orb}(K_i) = \{gK_ig^{-1} \mid g \in G\}.$$

また, K_i の固定群を $\mathrm{Stab}(K_i)$ と書く．すなわち,

$$\mathrm{Stab}(K_i) = \{g \in G \mid gK_ig^{-1} = K_i\}.$$

よく知られているように,

$$|\mathrm{Orb}(K_i)| = \frac{|G|}{|\mathrm{Stab}(K_i)|}.$$

Sylow の定理によれば, G のどの 2 つの Sylow 3 部分群も互いに共役であるから, $\mathrm{Orb}(K_i) = \Omega$. よって,

$$|\mathrm{Orb}(K_i)| = |\Omega| = 4.$$

さらに, $K_i \subseteq \mathrm{Stab}(K_i)$ であるから,

$$|K_i| \leq |\mathrm{Stab}(K_i)|.$$

ゆえに,

$$4 = |\mathrm{Orb}(K_i)| = \frac{|G|}{|\mathrm{Stab}(K_i)|} \leq \frac{|G|}{|K_i|} = 4.$$

これより, $|K_i| = |\mathrm{Stab}(K_i)|$ を得る．これと $K_i \subseteq \mathrm{Stab}(K_i)$ より, $K_i = \mathrm{Stab}(K_i)$ がいえる．したがって,

$$\ker\rho = \bigcap_{i=1}^{4} \mathrm{Stab}(K_i) = \bigcap_{i=1}^{4} K_i.$$

一方, 任意の異なる番号 i, j に対して, $K_i \cap K_j \subsetneq K_i$ が成り立つ．よって, $|K_i \cap K_j|$ は $|K_i|$ の真の約数である．$|K_i| = 3$ は素数なので, $|K_i \cap K_j| = 1$. すなわち, $K_i \cap K_j = \{e\}$. よって, $\ker\rho = \{e\}$. ゆえに, ρ は単射であり, $\rho(G)$ は S_4 の位数 12 の部分群である．一方, S_4 の位数 12 の部分群は A_4 しかない．したがって, G は A_4 と同型である． □

［**注意 7.3**］D_{12}, Q_{12}, A_4 はすべて同型ではない．実際, A_4 は位数 6 の元をもたないが, D_{12} と Q_{12} は位数 6 の元をもつ．また, D_{12} は位数 4 の元をもたないが, Q_{12} は位数 4 の元をもつ．