群論と対称性 – 位数 15 以下の有限群の分類

花木章秀 (信州大学)

April 19, 2023

このノートでは位数 15 以下の有限群の分類を与える。(位数 16 には 14 個の同型類があり、やや大変である。) 先に結果を書いてしまえば、以下の通りである。

位数	同型類		位数	同型類	
1	1		9	C_9, $C_3 \times C_3$	§2
2	C_2	p	10	C_{10}, D_{10}	§3
3	C_3	p	11	C_{11}	p
4	C_4, $C_2 \times C_2$	§2	12	C_{12}, $C_6 \times C_2$, D_{12}, Q_{12}, A_4	§6
5	C_5	p	13	C_{13}	p
6	C_6, S_3	§3	14	C_{14}, D_{14}	§3
7	C_7	p	15	C_{15}	§4
8	C_8, $C_4 \times C_2$, $(C_2)^3$, D_8, Q_8	§5			

この表で、「p」は素数位数のため巡回群しかないことを表し、その他は説明のある § を表している。

1　仮定する結果

定理 1.1 (Sylow の定理)**.** p を素数とする。$|G| = p^n m$, $p \nmid m$ とする。G の位数 p^n の部分群を G の *p-Sylow* **部分群**という。G の p-Sylow 部分群全体の集合を $\mathrm{Syl}_p(G)$ で表す。このとき次が成り立つ。

(1) $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$ (したがって $\mathrm{Syl}_p(G) \neq \emptyset$)

(2) G の p-Sylow 部分群は互いに G-共役である

$P \in \mathrm{Syl}_p(G)$ とするとき

$$P \trianglelefteq G \Longleftrightarrow |\mathrm{Syl}_p(G)| = 1$$

が成り立つ。また $N_G(P) = \{x \in G \mid x^{-1}Px = P\}$ (P の**正規化群**) とおくと $|\mathrm{Syl}_p(G)| = |G : N_G(P)|$ が成り立つ。$P \leq N_G(P)$ が成り立つので $|\mathrm{Syl}_p(G)| = |G : N_G(P)|$ は $|G : P|$ の約数である。

定理 1.2 (有限アーベル群の基本定理). A を有限アーベル群とする。ある自然数 r と $n_1, \ldots, n_r$ が一意的に存在し

$$A \cong C_{n_1} \times \cdots \times C_{n_r}, \quad n_{i+1} \mid n_i \quad (i = 1, \ldots, r-1)$$

となる。

これによって、位数が素数べき p^n のアーベル群の同型類は n の分割 (ヤング図形) に対応することが分かる。一般の位数の同型類は、素数毎に同型類を求め、その組み合わせとして記述される。

2 位数 p^2 の群 (p は素数)

p を素数とする。位数 p^2 の群を分類するために、より一般に、位数 p^n の群について考える。位数 p^n の群を (有限) p-**群**という。

補題 2.1. $a \in G$ に対して a を含む共役類 $a^G = \{g^{-1}ag \mid g \in G\}$ の元数は $|G : C_G(a)|$ である。ただし $C_G(a) = \{x \in G \mid ax = xa\}$ (a の**中心化群**) である。特に $|a^G|$ は $|G|$ の約数である。

また $|a^G| = 1$ であることと $a \in Z(G) = \{x \in G \mid xy = yx\ (\forall y \in G)\}$ (G の**中心**) は同値である。

G の共役類を $C_1, \ldots, C_k$ とし $C_1 = \{1\}$ とする。G は共役類に類別されるから

$$|G| = |C_1| + \cdots + |C_k|$$

となる。これを G の**類等式**という。$x_i \in C_i$ とすれば $|C_i| = |x_i^G| = |G : C_G(x_i)|$ であるから、各 $|C_i|$ は $|G|$ の約数である。

定理 2.2. p-群 $P\ (\neq 1)$ に対して $Z(P) \neq 1$ である。

証明. 類等式 $|G| = |C_1| + \cdots + |C_k|$ において $|G| = p^n$, $|C_1| = 1$ である。C_1 以外に $|C_i| = 1$ となる i が存在しないならば、類等式の右辺は p で割り切れず矛盾である。したがって $|C_i| = 1$ となる i が存在し $1 \neq x_i \in C_i$ は $Z(G)$ に含まれる。 □

定理 2.3. $G/Z(G)$ が巡回群であるならば G はアーベル群である ($G = Z(G)$ である)。

証明. $G/Z(G) = \langle xZ(G) \rangle$ とする。$a, b \in G$ とする。$a = x^i z$, $b = x^j z'$ となる $i, j \in \mathbb{Z}$, $z, z' \in Z(G)$ が存在する。よって $ab = x^i z x^j z' = x^j z' x^i z = ba$ となる。したがって G はアーベル群である。 □

系 2.4. 位数 p^2 の群はアーベル群である。したがって C_{p^2} または $C_p \times C_p$ と同型である。

証明. P を位数 p^2 の群とする。$Z(P) = G$ ならば P はアーベル群である。また $Z(P) \neq 1$ である。よって $|Z(P)| = p$ と仮定する。$Z(P)$ は P の正規部分群であり $P/Z(P)$ は位数が p なので巡回群である。したがって P はアーベル群、すなわち $Z(P) = P$ となり矛盾である。 □

3　位数 $2p$ の群 (p は奇素数)

p を奇素数とし、位数 $2p$ の群を考える。そのために、まず**二面体群** D_{2n} を定義する。
　n を $n \geq 3$ なる自然数とする。

$$D_{2n} = \langle a, b \mid a^n = b^2 = 1,\ ba = a^{-1}b \rangle = \{a^i b^j \mid 0 \leq i < n,\ 0 \leq j < 2\}$$

とおいて、これを位数 $2n$ の**二面体群**という。
　任意の $0 \leq i < n$ に対して

$$(a^i b)^2 = a^i b a^i b = a^i a^{-i} bb = 1$$

となり、$a^i b$ の位数は 2 である。

定理 3.1. p を奇素数とし $|G| = 2p$ とする。このとき G は C_{2n} または D_{2n} と同型である。

証明. G がアーベル群であるならば C_{2p} と同型である。G を非アーベル群とする。
　G は位数 p の元 a をもち $\langle a \rangle \trianglelefteq G$ である。$b \in G \setminus \langle a \rangle$ とする。b の位数 $o(b)$ は $2p$ の 約数であるから、$1, 2, p, 2p$ のいずれかである。$b \neq 1$ より $o(b) \neq 1$、$\mathrm{Syl}_p(G) = \{\langle a \rangle\}$ より $o(b) \neq p$、G が巡回群ではないから $o(b) \neq 2p$ である。よって $o(b) = 2$ である。$bab^{-1} = a^i$ となる i が存在する。$b^2 = 1$ より $a = b^2 ab^{-2} = ba^i b^{-1} = a^{i^2}$ となるから $i^2 \equiv 1 \pmod p$ である。$\mathbb{Z}/p\mathbb{Z}$ の乗法群は巡回群であるから、このような i は ± 1 しかない。$i = 1$ ならば G はアーベル群になるから $ba = a^{-1}b$ である。 □

　$S_3 \cong D_6$ であることに注意しておく。

4　位数 pq の群 (p, q は素数, $p \nmid q-1$, $q \nmid p-1$)

p, q を異なる素数とし $p \nmid q-1, q \nmid p-1$ とする。これは $p \not\equiv 1 \pmod q$, $q \not\equiv 1 \pmod p$ ということである。G を $|G| = pq$ である群とする。$P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$ とすれば、Sylow の定理から $P \trianglelefteq G$, $Q \trianglelefteq G$ である。よって、位数 p の元は P に含まれるもののみで $p-1$ 個ある。同様に、位数 q の元は $q-1$ 個ある。G の元の位数は $1, p, q$, pq のみであり、

$$1 + (p-1) + (q-1) = p + q - 1 < pq$$

であるから、G は位数 pq の元をもち、よって巡回群である。

定理 4.1. p, q を異なる素数とし $p \nmid q-1$, $q \nmid p-1$ とする。このとき位数 pq の群は巡回群 C_{pq} と同型である。

5　位数 8 の群

位数 8 の群を考える。まずアーベル群が C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$ のいずれかと同型であることが分かる。また次の定理はよく知られている。

定理 5.1. 群 G の単位元以外のすべての元の位数が 2 であるならば G はアーベル群である。

G を $|G|=8$ である非アーベル群とする。G に位数 8 の元があれば G は巡回群である。また位数 4 の元がなければ G はアーベル群となる。よって G は位数 4 の元 a をもち、指数が 2 であることから $\langle a\rangle \trianglelefteq G$ である。$b\in G\setminus\langle a\rangle$ とする。

$bab^{-1}\in\langle a\rangle$ なので $bab^{-1}=a^i$ となる i が存在する。$b^2\in\langle a\rangle$ であることから $a=b^2ab^{-2}=ba^ib^{-1}=a^{i^2}$ となる。$\mathbb{Z}/4\mathbb{Z}$ の乗法群は位数 2 の巡回群であるから、このような i は ±1 しかない。$i=1$ ならば G はアーベル群になるから $ba=a^{-1}b$ である。

$|G/\langle a\rangle|=2$ だから $b^2\in\langle a\rangle$ であり、したがって $b^2=a^s$ となる s が 4 を法として存在する。$s=1,3$ とすると b の位数が 8 となって G が非アーベル群であることに反する。よって $s=0$ または 2 である。

$s=0$ のときは G は二面体群 D_8 と同型である。$s=2$ のときは G は**四元数群**

$$Q_8=\langle a,b\mid a^4=1,\ b^2=a^2,\ ba=a^{-1}b\rangle=\{a^ib^j\mid 0\le i<4,\ 0\le j<2\}$$

と同型になる。Q_8 の位数 2 の元は a^2 のみであり、D_8 と非同型であることが分かる。

定理 5.2. 位数 8 の群は以下のいずれかの群と同型である。

$$C_8,\ C_4\times C_2,\ C_2\times C_2\times C_2,\ D_8,\ Q_8$$

6 位数 12 の群

まず、アーベル群は C_{12} または $C_6\times C_2$ である。G を非アーベル群とする。

- G は位数 6 の元 a をもつとする。このとき $\langle a\rangle\trianglelefteq G$ である。$b\in G\setminus\langle a\rangle$ とする。

  $bab^{-1}\in\langle a\rangle$ なので $bab^{-1}=a^i$ となる i が存在する。$b^2\in\langle a\rangle$ であることから $a=b^2ab^{-2}=ba^ib^{-1}=a^{i^2}$ となる。$\mathbb{Z}/6\mathbb{Z}$ の乗法群は位数 2 の巡回群であるから、このような i は ±1 しかない。$i=1$ ならば G はアーベル群になるから $ba=a^{-1}b$ である。

  $|G/\langle a\rangle|=2$ だから $b^2\in\langle a\rangle$ であり、したがって $b^2=a^s$ となる s が 6 を法として存在する。$b^2\in\langle a\rangle$ は b と可換だから、$x^s=b^{-1}x^sb=x^{-s}$ となり $s=0$ または 3 である。$s=0$ のときは二面体群 D_{12} で、$s=3$ のときは**一般四元数群**

  $$Q_{12}=\langle a,b\mid a^6=1,\ b^2=a^3,\ ba=a^{-1}b\rangle=\{a^ib^j\mid 0\le i<6,\ 0\le j<2\}$$

  と同型になる。Q_{12} は $a^3=b^2$ 以外に位数 2 の元をもたず、D_{12} と非同型であることが分かる。

- G は位数 6 の元 a をもたないとする。$P\in\mathrm{Syl}_2(G),\ Q\in\mathrm{Syl}_3(G)$ とする。$x\in Q$ とする。

  $C_G(x)\ne\langle x\rangle$ とし、$y\in C_G(x)\setminus\langle x\rangle$ とする。y の位数が 3 ならば $\langle x,y\rangle$ は位数 9 の部分群となり矛盾である。y の位数が 6 または 12 ならば、G が位数 6 の元 a をもたないことに反する。したがって y の位数は 2 または 4 となるが、このとき

xy の位数は 6 または 12 となり、やはり G が位数 6 の元 a をもたないことに反する。したがって $C_G(x) = \langle x \rangle$ であり、$|x^G| = |G : C_G(x)| = 4$ である。

$|\operatorname{Syl}_3(G)| = 1$ または 4 である。$|\operatorname{Syl}_3(G)| = 1$ とすれば $Q \trianglelefteq G$ であり、G は位数 3 の元を 2 つしかもたない。これは $|x^G| = |G : C_G(x)| = 4$ に反するので $|\operatorname{Syl}_3(G)| = 4$ である。G は位数 3 の元を 8 個もち、位数が 2 べきである元は高々 4 個である。P の元は位数が 2 べきなので、P は位数が 3 でない元のすべて、したがって正規部分群となる。

$1 \neq y_1 \in P$ を位数 2 の元とする。$xy_1x^{-1} = y_1$ ならば xy_1 の位数が 6 になるので $xy_1x^{-1} \neq y_1$ である。$y_2 = xy_1x^{-1}$ とおく。同様に $xy_2x^{-1} \neq y_2$ でるから $y_3 = xy_2x^{-1}$ とおく。$y_1 = y_3$ とすると $x^2y_1x^{-2} = y_1$ となり x^2y_1 が位数 6 の元となる。したがって $y_1 \neq y_3$ であり $P = \{1, y_1, y_2, y_3\}$ となる。y_1, y_2, y_3 はすべて位数が 2 となるので $P \cong C_2 \times C_2$ である。

$x \mapsto (1\ 2\ 3)$, $y_1 \mapsto (1\ 2)(3\ 4)$ と対応させることによって G が交代群 A_4 と同型であることが確認できる。

定理 6.1. 位数 12 の群はu以下のいずれかの群と同型である。

$$C_{12},\ C_6 \times C_2,\ D_{12},\ Q_{12},\ A_4$$

最後に $D_{12} \cong S_3 \times C_2$ であることに注意しておく。