群の抽象性と散在性―シローの定理と位数 12 の群 (第２版)

上野孝司

2017 年 1 月 5 日

群の抽象性と散在性－シローの定理と位数１２の群（第２版）

（共役と正規化群の概念を導入したうえで、シローの第２定理、第３定理の証明を追加した）

１. 概念で解く

高校までの数学では問題を解くうえで、なんらかの数学的技術を用いることが多い。三角関数の加法定理、数列の漸化式、積分の置換積分や部分積分などなど。大学受験では、これらの技術を正確かつ的確に用いる能力が求められる。

一方、大学の数学では、新しい概念を導入し、その概念を用いて問題を解くことが一般的である。時として、新しい概念は抽象的であり、それを数学の問題に適用する際に難しいと思われることがしばしばあり、それが高校数学と大学数学の決定的な違いとなる。その格差の大きさに嫌気がさして、高校までは得意であった数学の学習を大学で断念してしまうひとも多いようだ。解析学で、高校数学までは疑う余地のない関数の連続性を、大学で $\varepsilon - \delta$ 論法で厳密に定義し、連続性を再考するといった緻密な作業に戸惑った経験をされた方も多いと思われる。

筆者も高校数学と大学数学の格差に大きな戸惑いを覚えたひとりであるが、それでも新しい概念の新鮮さに魅せられ、逆に闘志を燃やして新たな数学に挑戦していった。新しい概念のなかでも筆者が特に興味を惹かれたのが、群論に出てくる、“**群の集合への作用**”というものであった。この概念から、群論のダイナミズムに改めて感じ入った。そして、この概念を用いて、有限群の位数に関する問題が見事に証明される、いわゆる「**シローの定理**」に触れたときは、その巧妙ではあるが、証明の美しさに感動した衝撃を今でも覚えている。これまでの技術による証明とは異なり、“概念で解く”という大学数学を表象する新たな体験に大いに精神が躍動したのであった。

２．群の個別散在性

シローの定理を述べる前に、群論を特徴づける群の**個別散在性**について触れておこう。

群論のなかの一大領域に有限群論というものがある。有限群の位数や構造を分析する分野である。群の種類としては、ざっと頭に浮かぶものを挙げると、

＊巡回群、可換群（アーベル群)、対称群（置換群)、交代群、剰余類群、単純群、正多面体群、四元数群、可解群

などが挙げられる。いずれも独立した概念であるが、相互に関連しあっている。有限群論の初歩は、まずは 与えられた自然数 n に対して、位数 n の部分群は何種類あり、どのような構造を持つか を研究する。その基本は、

（＊）位数が素数である群は、巡回群である。

というものであろう。これより、位数が、３、５、７、11、・・・・・などの素数の群は巡回群である。次に位数４の群が基本的であり、これは、

巡回群、クラインの４元群

の二つからなる。位数４の群の分類は比較的簡単だが、位数８、12 の群となると一気に複雑化する。

＊位数８の群：５種類

巡回群（C_8), $C_4 \times C_2$, $C_2 \times C_2 \times C_2$

２面体群 D_8, ４元数群 Q_8

＊位数 12 の群：５種類

巡回群（C_{12}), $C_6 \times C_2$, ２面体群 D_{12}, 四元数群 Q_{12}, ４次の交代群 A_4

なお、数学辞典（岩波書店）によると、位数 n に対する群の種類の数については、以下の表のような対応となる。

位数 n	8	12	16	18	20	24	27	28	30	32	60
群の個数	5	5	14	5	5	15	5	4	4	51	13

また、有限単純群については、以下のことがわかっている。

＊単純群の４つのタイプ

(1) 素数 p の巡回群

(2)$n \geqq 5$ のときの交代群 A_n

(3) 有限体上の線形群から得られるリー型と呼ばれる単純群

(4) 散在的単純群 26 個

以上みてきたように、群の位数とその構造、種類は非常に個別散在的であることがわかるであろう。たった４つの群の公理（演算・結合法則・単位元・逆元）だけで、これだけ散在的な事象が多くみられることは、人知を越えた神の仕業のようであり、一種異様な感すら覚える。

一方、群の部分群の位数については、次節で解説するシローの定理が知られており、基本的かつ極めて重要であり、群の分類に際して有用である。。上述の個別散在的な事象とは対照的に、非常に一般的、抽象的な論理展開となっており、その美的ともいえる奇抜性に読者は驚かれることであろう。本稿では群の抽象性の象徴ともいえるシローの定理と個別散在性の両面を述べる。

３．シローの定理

3.1．群の集合への作用

本節では、シローの定理の準備として、“**群の集合への作用**”という概念を説明する。これはそれ自体独立した概念であり、応用範囲が広くその具体的事例のひとつがシローの定理である。

【群の集合への作用】

G を群、M をひとつの集合とする。M は群である必要はなく、文字通りひとつの集合ととらえていただきたい。M が具体的に決まっていないと落ち着かないひともいるかもしれないが、現代数学はできるだけ応用範囲を広くするため議論を可能な限り広く一般化して扱う。このため話が抽象的になる傾向があるが、その方が逆に議論の本質がみえてくるのである。後に説明する具体例で概念をイメージしてとらえることができるだろう。

群 G が集合 M へ作用するとは、G の各元 g に対して、$x \in M$ に対して、M から M への写像 φ_g

$\varphi_{g;} : M \ ------> M$

$\quad x \ ------> g(x)$ が決まり、以下の条件を満たすことをいう。

（1）$g_1(g_2(x)) = (g_1 g_2)(x)$

（2）G の単位元 e に対して、$e(x) = x$

つまり、φ_g は M へ作用して、M の元を M の元に移す。

（ただし、G の単位元は M の元を動かさない）

(1),(2) より、群の集合への作用 φ_g は、M から M への全単射、つまり、一対一に対応していることが簡単にわかる。全射（M から M の上への写像) であることは、任意の $x \in M$ に対して、

$g(g^{-1}(x)) = (gg^{-1})(x) = x$

であることからわかる。単射であることは、

$x_1, x_2 \in M$ に対して、

$\quad g(x_1) = g(x_2)$ のとき、両辺に g^{-1} を作用させると、

$(g^{-1}g)(x_1) = (g^{-1}g)(x_2)$

から、$x_1 = x_2$ が成り立つことから明らかある。

３．２ 軌道と固定部分群

G を群、M を集合とし、G から M への作用 φ_g を考える。

$\varphi_g : M \ ------> M$

$\quad x \ ------> g(x)$

いま、$x_0 \in M$ をひとつとり、これを固定して考える。

このとき、M の部分集合 $G(x_0)$ を、

$G(x_0) = \{g(x_0) | g \in G\}$

$\quad = \{g_1(x_0), g_2(x_0), \cdots\cdots, g_n(x_0), \cdots\cdots\}$

とする。つまり、固定された M の元 x_0 に G を連続的に作用させて得られる M の部分集合を $G(x_0)$ と定義するのである。この $G(x_0)$ を M の元 x_0 の G による**軌道**または $G-$ 軌道とよぶ。

［例］G を、$\begin{bmatrix} \cos\frac{\pi}{3}n & -\sin\frac{\pi}{3}n \\ \sin\frac{\pi}{3}n & \cos\frac{\pi}{3}n \end{bmatrix} = T_n$（$n$ は整数）

なる 2×2 行列 T_n からなる群（演算は通常の積）とする。

$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ は、θ の回転を表すから、T_n は、$(60^\circ \times n)$ 回転する $\mathbb{R}^2$ から $\mathbb{R}^2$ への線形作用素の集合からなる群である。

$M =$ 半径 1 の円周の点からなる集合とする。

このとき、$\alpha = \begin{pmatrix} x \\ y \end{pmatrix} \in M$ とすると、

群 G の集合 M の作用、$\varphi_{T_n} = T_n\alpha$

は、α を $(60\times n)^\circ$ 回転した点に移す。容易にわかるように、α の軌道 $G(\alpha)$ は、

$\{\alpha, T_1\alpha, T_2\alpha, T_3\alpha, T_4\alpha, T_5\alpha\}$ と正６角形の頂点となる。この例で、群の集合への作用や軌道といった概念を具体的にイメージできるだろう。円周上にパッと花が咲き、それがくるくると回転するようなイメージである。

軌道については、次の重要な事項が成り立つ。

$M = \bigcup_x G(x) = G(x) \cup G(y) \cup G(z) \cup \cdots\cdots$

（証明）$y \notin G(x) \Longrightarrow G(x) \cap G(y) = \varnothing$

もし、$G(x) \cap G(y) \neq \varnothing$ ならば、

$\exists z \in M \quad z \in G(x) \cap G(y)$

より、$\exists g, h \in G \quad z = g(x) = h(y)$

より、$h^{-1}g(x) = y$

となるから、$y \in G(x)$ となり、仮定に矛盾する。

いま、$z \notin G(x) \cap G(y)$ とすると、

$G(x) \cup G(y) \cup G(z) \cdots\cdots$

と次々に M の元の G 軌道の和集合を考えていくと、

$$M = \bigcup_x G(x)$$

となる。■

次に軌道と関連した概念である**固定部分群**について述べる。

群 G が集合 M へ作用するとして、固定された $x_0 \in M$ に対して、G の部分群 G_{x_0} を、

$G_{x_0} = \{g \in G |\ g(x_0) = x_0\}$

で定義する。つまり、x_0 への作用を不動とするような $g \in G$ の集合を G_{x_0} とするのである。以下に示すように G_{x_0} は群（G の部分群）となり、これを x_0 の固定部分群と呼ぶ。部分群になることは、以下のようにしてわかる。

$g, h \in G_{x_0}$ とするとき、$(gh)(x_0) = g(h(x_0)) = g(x_0) = x_0$

より、$gh \in G_{x_0}$

また、任意の $x_0 \in M$ に対して、

$x_0 = (g^{-1}g)(x_0) = g^{-1}(g(x_0)) = g^{-1}(x_0)$

より、$g^{-1} \in G_{x_0}$

となる。■

群 G が集合 M へ作用するとき、$x_0 \in M$ の G 軌道 $G(x_0)$ と固定部分群 G_{x_0} については、以下の重要な定理が成り立つ。

【定理】

群 G が集合 M へ作用するとき、

$$|G| = |G(x_0)| \times |G_{x_0}|$$

（証明）

$G(x_0) = \{x_0, x_1, x_2, \cdots\cdots, x_{s-1}\}$ (s 個)

とする。すると、$G(x_0)$ の定義より、各 $x_i (i = 1, 2, \cdots, s-1)$ に対して、

$g_i(x_0) = x_i$　となる g_i が存在する。

いま、$g_i'(x_0) = x_i$　とするとき、

$$\begin{aligned} x_0 &= g_i^{-1}(x_i) \\ &= g_i^{-1}(g_i'(x_0)) \\ &= g_i^{-1}g_i'(x_0) \end{aligned}$$

よって、$g_i^{-1}g_i' \in G_{x_0}$ となり、これより、$g_i' \in g_iG_{x_0}$

つまり、g_i' と g_i は G_{x_0} の同じ左剰余類に入る ことがわかる。

以上から、$G(x_0) = \{x_0, x_1, x_2, \cdots\cdots, x_{s-1}\}$ で、$g_ix_0 = x_i$ なる g_i をそれぞれひとつとるとき、

$G = G_{x_0} + g_1G_{x_0} + g_2G_{x_0} + \cdots\cdots + g_{s-1}G_{x_0}$

よって、

$|G| = |G_{x_0}| \times s(x_0$ の軌道の元の個数$) = |G_{x_0}| \times |G(x_0)|$

以上より、x_0 の G 軌道と、G の G_{x_0} による左剰余類による集合とが一対一に対応する ことがわかる。■

3.3 シローの定理

これまで述べてきた群の集合への作用、軌道、固定部分群の概念を用いてシローの定理（シローの第１定理）を証明する。

【定理】シローの第１定理

G を有限群とする。$|G|$ の素因数のひとつをp(素数）とし、$|G|$ を割り切るp の最大のべき数をp^m とする。このとき、G には位数p^m の部分群が存在する。

（証明）以下は、Wielandt 論法とよばれる巧妙な証明法である。

$|G| = kp^m$　とおく。p^m は素因数 p の最大のべき数で、$(k, p) = 1$ である。いま、G の部分集合からなる集合 M を、

$M =$ 元の数が p^m 個からなる G の**部分集合からなる集合**とする。

$$|M| = \begin{pmatrix} kp^m \\ p^m \end{pmatrix}$$

このとき、$\begin{pmatrix} kp^m \\ p^m \end{pmatrix}$ **はp と互いに素である・・・・・(∗)**

が成り立つ（証明略）。

いま、G の M への作用を、$A \in M,\ g \in G$ として、

$gA \equiv \{gx \mid x \in A\}$ (gx は群の演算としてすでに定義されている）とする。

$x - - - \succ gx$　は一対一対応であるから、gA もまた元の個数が p^m である M の元である。

$gA \in M(A \in M, g \in G)$

さて、M を A の G 軌道 $G(A)$ によって分解してみよう。このとき、すべての G 軌道が p の倍数となることはない。なぜなら、

$$M = \bigcup G(A)$$

であるから、すべての軌道が p の倍数となるならば、$|M| = \begin{pmatrix} kp^m \\ p^m \end{pmatrix}$ が p の倍数となり、

$\begin{pmatrix} kp^m \\ p^m \end{pmatrix}$ が p と互いに素 $\cdots\cdots$（∗）

であることに反する。

$M = \bigcup_A G(A) = G(A) \cup G(B) \cup G(C) \cdots\cdots\cdots\cdots$

s 個　　t 個　　u 個

$s, t, u, \cdots\cdots$ すべてが p の倍数となることはない.

$|G(A)|$ **が**p **と互いに素であるような**A **が存在する**。この A に注目し、A を固定して考えよう。

すると、上述の軌道と固定部分群の関係を $G(A), G_A$ に適用すると、

$$|G| = |G(A)| \times |G_A|$$

が成り立つ。$(|G(A)|, p) = 1,\ \ |G| = kp^m$ より、

$|G_A|$ **は**p^m **の倍数でなければならない。**

よって、

$|G_A| \geqq p^m \cdots\cdots\cdots (1)$

が成り立つ。一方、A の元 x_0 をひとつ固定して対応

$$G_A \ni g - - - - - > gx_0 \in A$$

を考える。$g \neq g'$ ならば、$gx_0 \neq g'x_0$　より、

$|G_A| \leqq A$ の元の個数$= p^m \cdots\cdots\cdots (2)$

よって、$(1), (2)$ より、$|G_A| = p^m$　■

シローの定理から直ちに次の 2 つの系が導かれる。

系 1．p が素数で、$P||G|$(G の位数が p で割り切れる）ならば、G は位数 p の元を含む.

系 2．p を $|G|$ の素因数として、$|G| = p^e s, (p, s) = 1$ とすれば、G は位数 p^e の部分群（$p-$ **シロー群**という）を持つ。

なお、以下にシローの第 2 定理、第 3 定理とよばれる定理を述べる。以下の群の分類で重要な役割」を果たす。

【定理】

G を有限群として、p を $|G|$ のひとつの素因数とする。このとき、次の定理が成り立つ。

(1)G の任意の p 部分群（位数が p のべきであるような部分群）は、G のある p-シロー部分群に含まれる。

(2)**（シローの第 2 定理）**G の任意の 2 つの p-シロー群は G において**共役**である。

＊群 G の部分群 H に対して適当な G の元 g をとると、gHg^{-1} と表せる部分群を H に共役な部分群であるという。

(3)**（シローの第 3 定理）**G **の**p**-シロー部分群の個数は 1 +**kp **の形をし、しかもそれは、**$|G|$ **の約数である。**

以下、この定理を証明する。そのための準備として、**共役**と**正規化群**の概念を導入したうえで、群の第 2 同型定理について述べる。

・G を群とし、a, b を G の元とする。$sas^{-1} = b$ となるような G の元 s が存在するとき、a は b に共役 であるという。共役は G におけるひとつの同値関係となる。G を共役関係によって類別したときの各類を G の共役類という。

・共役の概念は G の部分集合の間にも定義することができる。すなわち G の部分集合 S, S' に対して、$aSa^{-1} = S'$ となるような G の元 a が存在するとき、S は S' に共役である という。これは G の部分集合の間の同値関係である。G の部分群 H に共役な集合 aHa^{-1} はまた G の部分群となる。これを H の共役部分群という。

・G を群、H を G の部分群とする。G の部分集合 A, B に対して $xAx^{=1} = B$ となる $x \in H$ が存在するとき、A, B は“H に関して共役”であるという。この関係は明らかに G の部分集合の間の同値関係である。

・a を G の 1 つの元とする。そのとき $N(a) = \{x | x \in G, ax = xa\}$ は G の部分群となることは容易にわかり、これを G における a の**正規化群**という。

【補題 1】 G を有限群とする。そのとき、G の元 a の共役類に含まれる元の個数は $(G : N(a))$ に等しい。

（証明略）

【補題 2】 S を群 G の部分集合とし、$N(S)$ を G における S の正規化群とする。そのとき、S に共役な G の異なる部分集合の個数は $(G : N(S))$ に等しい。

（証明略）

【補題 3】 G を有限群、H を G の部分群とする。そのとき、G の与えられた部分集合 A と H に関して共役な集合の個数は $(H : H \cap N(A))$ に等しい。これは、補題 2 の一般化である。

（証明略）

【定理（第 2 同型定理）】 G を群、N を G の正規部分群、H を G の任意の部分群とする。そのとき HN は G の部分群、$H \cap N$ は H の正規部分群で、

$$H/(H \cap N) \cong HN/N$$

が成り立つ。（証明略）■

以上の準備のもとに上の定理 (シローの第 2 定理、第 3 定理）を証明しよう。以下の証明は、『代数系入門』(松坂和夫）によった。

[証明]$|G| = p^e s, (p, s) = 1$ とし、P を G の一つの $p-$ シロー部分群とする。P に共役な G の部分群全部の集合を $\mathcal{P}$ とし、$\mathcal{P}$ の元の個数を s' とする。$s' = (G : N(P))$ であるから（補題 2）、s' は $|G|$ の約数である。また $N(P) \supset P$ であるから、s' は $(G : P) = s$ の約数で、したがって p と互いに素である。

いま、H を任意に与えられた G のひとつの p 部分群とする。そのとき $\mathcal{P}$ の元を H に関して互いに共役であるものに分類することができる。$\mathcal{P}$ の H に関する共役類を $\mathcal{P}_1, \cdots, \mathcal{P}_t$ とし、P を含む共役類を $\mathcal{P}_1$ とする。また、各共役類 $\mathcal{P}_i (1 \leqq i \leqq t)$ の元の個数を a_i, 各 $\mathcal{P}_i$ から任意にとった 1 つの代表を P_i とする。このとき、

$$s' = a_1 + \cdots + a_t$$

で、また補題 3 により $a_i = (H : H \cap N(P_i))$ である。したがって、a_i は $|H|$ の約数であるから、p のべき ($P^0 = 1$ の場合を含む）であるが、s' は p と互いに素であるから、$a_1, \cdots .a_t$ のうちに 1 となるものが必ず存在する。$a_i = 1$ であることは $H \subset N(P)$ を意味するが、$N(P_i)$ においてその正規部分群 P_i と部分群 H に対して定理（第 2 同型定理）を適用すれば、$(HP_i : P_i) = (H : H \cap P_i)$ が得られる。この左辺は $(G : P_i) = s$ の約数で、右辺は p のべきであるから、この値は 1 に等しく、したがって $H \subset P_i$ でなければならない。これで H をふくむ $p-$ シロー群の存在が示された。

次に、P' を G の任意の $p-$ シロー部分群とし、上記の H として P' をとる。そのとき、上述から $P' \subset P_i$ となる P_i が存在するが、両者の位数は等しいから $P' = P$ でなければならない。ゆえに P' は P と共役である。

最後に、上の H として P 自身をとる。そのとき、(P の P 自身に関する共役部分群は P のみであるから)、$a_1 = 1$ である。一方、$2 \leqq i \leqq t$ である各 t に対して $P \neq P_i$ であるから、a_i は 1 に等しくない p のべきである。(もし $a_i = 1$ ならば上に示したように $P \subset P_i$ となる。) ゆえに $a_2 + \cdots + a_t$ は P の倍数となり、したがって、$s' = 1 + kp$ の形となる。しかもはじめに述べたように s' は $|G|$ の約数である。これでシローの第 3 定理が証明された。■

４．群の類別

群の類別の問題は、有限群論を学ぶうえで中心的な課題である。与えられた数を位数とする群にはどのような構造を持ったものが存在するかを類別する問題である。種類には、巡回群、可換群、対称群（置換群)、交代群、２面体群、四元数群など様々なものが存在する。例えば、位数８の群には、

C_8(巡回群）, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, ２面体群、四元数群

の５種類が存在する。

特に位数が 20 以下と比較的位数が小さい群の分類は初等的な群論を学ぶうえで避けては通れない問題である。しかし、専門家は別として、群論の入り口にいる者にとっては、これだけでもなかなか厄介な問題である。その際に基本的事項として、前述のシローの定理が効いてくる。

実は群の類別の問題は筆者にとって忘れがたい思い出がある。大学の数学科に進学したときの群論の演習(学部２年の後期課程）の初回で出題されたのが、“**位数 12 の群を類別せよ**”という問題であった。当時の東大数学科では、代数学では、岩堀長慶、飯高茂先生が担当され、演習には、当時助手だった川又雄二郎（位数 12 の問題の出題者、現東大教授)、加藤和也先生（現シカゴ大学教授、東大名誉教授）といった天才ぞろいのスーパースターの布陣となっていた。群の類別には、シローの定理を基本的定理として繰り返し用いるのであるが、シローの定理を学習していない初期の段階での出題にはいささか違和感を覚えた。私には手も足も出ない難問に映ったが、数学科全体でもこの問題をすんなり解けた学生はそれほど多くなかったと記憶している。

話が横道にそれたので主題に戻ろう。本稿では、位数 pq の群（p, q は素数)、位数８の群、位数 12 の群の類別を扱う。本論に入る前にいくつかの補題と２面体群、四元数群の定義を述べておく。なお、以下（特に第７節の（2)）は、ネット上の論文『小さい位数の群の分類』(2013.8．19　作者不詳）に沿っている。多少疑問と思われる部分があったので、例証を加えるなど反芻、咀嚼・消化して筆者なりの見解を述べたものである。

＊補題１.

G を群、A, B を G の部分群とし、

$|G| = |A||B|$　　$\gcd(|A|, |B|) = 1$(gcd は最大公約数、つまり、$|A|.|B|$ が互いに素）のとき、

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

＊補題２.

G を群、$a, b \in G$ とするとき、

$bab^{-1} = a^i$ ならば、

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

＊補題３.

G を群、任意の $x \in G$ に対して、$x^2 = e$ が成り立つとき、

G は可換群となる。

＊補題４.

G を群、H を G の部分群とするとき、

$(G : H) = 2$ ならば、

$H \lhd G$(正規部分群)

［補題の証明］

＊補題１.

$X \in A \cap B$ とする。$x \in A$ より、x の位数は $|A|$ の約数である。同様に x の位数は $|B|$ の約数である。ところが、$\gcd(|A|, |B|) = 1$　だから、$x = e$, ゆえに、$A \cap B = \{e\}$

さらに、$|AB| = \dfrac{|A||B|}{|A \cap B|} = |A||B|$

これと、$AB \subseteq G$ であるから、$G = AB$ を得る。

＊補題２.

n に関する数学的帰納法を用いる。

n のとき、$b^n a b^{-n} = a^{i^n}$　が成立するとき、

$b^{n+1} a b^{-(n+1)} = b b^n a b^{-n} b^{-1} = b a^{i^n} b^{-1} = (bab^{-1})^{i^n} = (a^i)^{i^n} = a^{i^{(n+1)}}$

＊補題３.

G の元 x, y を任意にとる。

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

であるから、$x^{-1} = x,\ y^{-1} = y,\ (xy)^{-1} = xy$

ゆえに、$yx = y^{-1}x^{-1} = (xy)^{-1} = xy$

＊補題４.

$x \in G$ を任意にとる。$xH = Hx$ であることを示せばよい。

$x \in H$ 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、$(G : H) = 2$ であるから、

$G = H \cup xH$

同様に右剰余類について、

$G = H \cup Hx$

よって、　$H \cup xH = H \cup Hx$

さらに、一般に異なる同値類は交わらないから、

$H \cap xH = H \cap Hx = \varnothing$

いま、$y \in xH$ とすると、$y \in H \cup xH = H \cup Hx$ よって、

$y \in H$　または、$y \in Hx$. もし仮に $y \in H$ とすると、$y \in H \cap xH = \varnothing$　となり、矛盾するから、$y \notin H$　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。■

■ ２面体群と四元数群

ここで、群の類別に際して基本的な２面体群と四元数群の定義を述べておく。

（1）整数 $n \geqq 3$ に対して、２つの生成元 a, b と基本関係

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

によって定義される群は位数 $2n$ の非アーベル群である。これを位数 $2n$ の**２面体群**といい、D_{2n} で表す。

（２）整数 $n \geqq 2$ に対して、２つの生成元 a, b と基本関係

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

によって定義される群は位数 $4n$ の非アーベル群である。これを位数 $4n$ の**四元数群**といい、Q_{4n} で表す。

５．位数pq の群（p, q は素数）

【定理５－１】

p, q を素数、$p > q$ かつ、$p \equiv 1(\mathrm{mod}\, q)$ ではないとき、

位数 pq の群は巡回群で、C_{pq} に同型である。

（証明）シローの定理より、G の $p-$ シロー群の個数を k_p とするとき、k_p は pq の約数かつ $k_p \equiv 1(\mathrm{mod} p)$ であるから、前者より、$k_p = 1, p, q, pq$ のいずれかであり、後者の条件より、$k_p = 1$ となって、G の $p-$ シロー群はただひとつ存在し、これを A とおく。

再び、シローの定理より、G の $q-$ シロー群の個数を k_q とするとき、k_q は G の位数の約数であるから、$1, p, q, pq$ のいずれかであるが、$k_q \equiv 1(\mathrm{mod}\, q)$ であるが、$p \equiv 1(\mathrm{mod}\, q)$ ではないから、$k_q = 1$.　よって、G の $q-$ シロー群はただひとつ存在し、それを B とおく（巡回群）。

$|G| = |A||B|$,　$\gcd(|A|, |B|) = 1$ であるから補題１より、$G = AB, A \cap B = \{e\}$,　$A, B \lhd G$ より、

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

【定理５－２】

p, q を素数、$p > q$ とする。このとき

$p \equiv 1(\mathrm{mod}\, q)$ が成り立つとすると、

合同方程式 $x^q \equiv 1(\mathrm{mod}\, p)$ の整数解$i_0 (2 \leqq i_0 \leqq p-1)$ が存在する。

このとき、位数 pq の群は、以下の２種類のいずれかである。

（1）$G \simeq C_{pq}$

（2）G は、$a^p = b^q = e, bab^{-1} = a^{i_0}$ なる非アーベル群に同型

（証明）G の $p-$ シロー群の個数を k_p とすると、k_p は $|G| = pq$ の約数かつ、$k_p \equiv 1(\mathrm{mod}\, p)$,

$p > q$ より、$k_p = 1$. この $p-$ シロー群を A とするとき、$A \lhd G$, 巡回群。A の生成元を a とおく。

$A = < a >$

再び、シローの定理より、G の $q-$ シロー群 B が存在する。$|B| = q$, 巡回群。B の生成元を b とおく。$B = < b >$

$|G| = |A||B|$,　$\gcd(|A|, |B|) = 1$ より、

$G = AB$,　$A \cap B = \{e\}$

$G = < a, b >$となる。

$A \lhd G$ ゆえ、$bab^{-1} = a^i (0 \leqq i \leqq p-1)$ なる i が存在する。

一方、$b^q = e$ であるから、$a = b^q a b^{-q} = a^{i^q}$ より、

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

このとき、 $i^q \equiv 1(\mod p)$ について、$p \equiv 1(\mod q)$ が成立するとき、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（１を含む）を持つ。その１以外の整数解をi_0 とすると、

$1, i_0, i_0^2, \cdots\cdots\cdots, i_0^{q-1}$ **が法p の整数解となる。**この整数に関する事象（合同方程式）が位数 pq の群の類別に際して、重要な役目を果たす。

（1）$i = 1$ のとき、$ba = ab$　よって G はアーベル群となる。このとき、

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

ここで、最後に $(p, q) = 1$ を用いた。

（2）$i \neq 1$ のとき、

G は、$a^p = b^q = e,\ bab^{-1} = a^{i_0}$ なる非アーベル群に同型となる。ひとつの解に基づく類別は、他の解による類別に同型となる（証明略）。■

[例１] 位数 15 の群

$15 = 3 \times 5 (p = 5, q = 3)$

$p = 5, 5 \equiv 1(\mod 3)$ ではないから、位数 15 の群は巡回群 C_{15}

[例２] 位数 35 の群

$35 = 5 \times 7 (p = 7, q = 5)$

$p = 7, 7 \equiv 1(\mod 5)$ ではないから、位数 35 の群は巡回群 C_{35}

[例３] 位数 21 の群

$21 = 3 \times 7 (p = 7, q = 3)$

$p = 7, 7 \equiv 1(\mod 3)$

$i^3 \equiv 1(\mod 7)$ の解は、$i = 1, 2, 4$

i	0	1	2	3	4	5	6
i^3	0	1	8	27	64	125	216
$mod7$	0	1	1	6	1	6	6

よって、$G \simeq C_{21}$ または、$a^7 = b^3 = e, bab^{-1} = a^2$ なる非アーベル群

[例 4] 位数 $2p$ の群（p は 3 以上の素数）

$p \equiv 1(\mod 2)$

$i^2 \equiv 1(\mod p)$ となる整数解として、$p - 1$ が存在する（$(p-1)^2 = p^2 - 2p + 1 \equiv 1(\mod p)$）

よって、$G \simeq C_{2p}$　または、$a^p = b^2 = e, bab^{-1} = a^{p-1}$ なる 2 面体群 D_{2p}

[例５] 位数 10 の群

$10 = 2 \times 5 (p = 5, q = 2)$

$p = 5 \equiv 1(\mod 2)$

$i^2 \equiv 1(\mod 5)$ の解は、１、４

i	0	1	2	3	4
i^2	0	1	4	9	16
$\mod 5$	0	1	4	4	1

よって、$G \simeq C_{10}$ または、$a^5 = b^2 = e, bab^{-1} = a^4$ なる 2 面体群（D_{10}）

[例６] 位数 55 の群

$55 = 5 \times 11 (p = 11, q = 5)$

$11 \equiv 1(\mod 5)$

$i^5 \equiv 1 (\mathrm{mod}\, 11)$ の整数解として、$i = 1, 3, 4, 5, 9$

i	1	2	3	4	5	6	7	8	9	10
i^5	1	32	243	1024	3125	7776	16807	32768	59049	100000
$\mathrm{mod}\, 11$	1	10	1	1	1	10	10	10	1	10

よって、$G \simeq C_{55}$ または、$a^{11} = b^5 = e, bab^{-1} = a^3$ なる非アーベル群

６．位数８の群

（１）G がアーベル群のとき、

(1) - 1 G が位数８の元を持つとき、$G \simeq C_8$

(1) - 2 G が位数４の元を持つとき、

a を位数４の元とし、$A =< a >$ とする。このとき、$b \notin A$ が存在する

（ア）b の位数 $= 2$ の場合

$G \simeq C_4 \times C_2$

（イ）b の位数$= 4$ の場合、b の位数２の場合に帰する（証明略）

(1) - 3 G が位数２だけの元（単位元以外）を持つとき

$G \simeq C_2 \times C_2 \times C_2$

(2) G が非アーベル群の場合

G の単位元以外の元の位数は、２または４であるが、

G は必ず位数４の元を持つ（すべての位数２ならば可換群となる）

そのひとつを a とし、$A =< a >$ とする。$|A| = 4$

A に属さない G の元を b とする。$G =< a, b >$

$A \lhd G$（正規部分群）($\because (G : A) = 2$）だから、

$bab^{-1} = a^i (0 \leqq i \leqq 3)$ なる i が存在する。

(2) - 1 $b^2 = e$ の場合、

$a = b^2ab^{-2} = a^{i^2} \Longrightarrow a^{i^2-1} = e$

これを満たすのは、$i = 1$ または 3

ところが $i = 1$ の場合は、$ba = ab$ と可換となり、仮定に反する。よって、$i = 3$

このとき、$a^4 = b^2 = e,\ ba = a^3b$　　これは２面体群 D_8 である。

(2) - 2 $b^2 \neq e$ の場合、

$A \lhd G, b \notin A$ であるから、$(G : A) = 2$ より、

$G = A \cup Ab$ となる。このとき、$b^2 \in A$ となるから、

$b^2 = a^i (0 \leqq i \leqq 3)$　なる i が存在する。

b の位数$= 2$ または４

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

a の位数 $= 4$ だから、$2i$ は４の倍数、つまり、i は２の倍数

よって、$i = 0$ または２　ところが $i = 0$ の場合は仮定に反するから $i = 2$ となる。$b^2 = a^2$

このとき、$bab^{-1} = a^j$　が成立する j を求めよう。

$(b^2)^2 = (a^2)^2 = a^4 = e$

よって、$b^4 = e$

$a = b^4ab^{-4} = a^{j^4} \Longrightarrow j^4 \equiv 1 (\mathrm{mod}\, 4)$

これを満たすのは、$j=3$($j=1$ のときは、可換となるから不可）

j	0	1	2	3
j^4	0	1	16	81
$\bmod 4$	0	1	0	1

よって、$a^4=e, b^2=a^2, bab^{-1}=a^3$　これは、四元数群 Q_8

以上をまとめると、位数８の群は、

$C_8,\ C_4\times C_2,\ C_2\times C_2\times C_2$　，２面体群 D_8，四元数群 Q_8 の５種類に類別される。■

７．位数 12 の群

（1）アーベル群の場合

G を位数 12 のアーベル群とする。シローの定理より、G の２‐シロー群 H および３‐シロー群 K が存在する。１２$=2^{\ 2}\times 3$ より、$|H|=4, |K|=3$ であり、

$|G|=|H||K|,\ \gcd(|H|,|K|)=1$　　であるから、補題１より、

$G=H\times K,\ H\cap K=\{e\}$

が成り立つ。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。

$G\simeq H\times K$

H の位数は 4 だから、$H\simeq C_4$(巡回群）または、$H\simeq C_2\times C_2$(クラインの四元群）である。

また、K の位数は３だから、$K\simeq C_3$(巡回群)。よって、位数 12 のアーベル群は、

$G\simeq C_4\times C_3\simeq C_{12}$, または　$G\simeq C_2\times C_2\times C_3\simeq C_2\times C_6$

（２）非アーベル群の場合

まず、シローの定理を使って、３‐シロー部分群を考える。３‐シロー部分群の個数を k とおくと、シローの定理より、$k\equiv 1(\bmod 3)$ かつ k は 12 の約数であるから、$k=1$ または 4 である。

（2）‐１　　$k=1$ のとき、

G には位数６の元が存在する（この証明はやや複雑な知識を要するので省略する)。その位数６の元を a とし、$A=<a>$ とおく。$|A|=6$ であるから、補題４より、$A\lhd G$ であることに留意されたい。A に含まれない G の元が存在するからそのひとつを b とする。$B=<b>\ (b\in G, b\notin A)$ とする。このとき、$G=<a,b>$ となる。

（2）‐１‐１　　$b^2=e$ の場合、$bab^{-1}=a^i(0\leqq i\leqq 5)$ とおけるから、補題２より、

$b^2ab^{-2}=a^{i^2}$　が成り立つが、$b^2=e$ であるから、

$a=a^{i^2}\Longrightarrow a^{i^2-1}=e$　よって、

$i^2\equiv 1(\bmod 6)$

これを満たす i は、$i=1$ または 5 であるが、$i=1$ のとき G は可換群となってしまうから仮定に反する。よって、$i=5$ となる。$bab^{-1}=a^5\Longrightarrow ba=a^5b$

以上より、$a^6=e, b^2=e, ba=a^5b$　　これは２面体群 D_{12} となる。

（2）‐１‐２　　$b^2\neq e$ の場合、

このとき、$b^2\in A$ となることが次のようにわかる。

$b^2\notin A$ ならば、$b^2\in Ab$ となり、$b^2=hb$ となる $h\in A$ が存在するが、このとき、

$b=h$ となり、$b\notin A$ に反する。よって、$b^2\in A$ となる。よって、

$b^2=a^i(1\leqq i\leqq 5)$ なる i が存在する。

＊$i=1$ とすると、$b^2=a$ となるが、$(b^2)^6=a^6=e$ より、$b^{12}=e$ となり、

G は巡回群となるから仮定（非アーベル群）に反する。

＊ $i=5$ とすると、

$(b^2)^6=(a^5)^6=(a^6)^5=e$ より、$b^{12}=e$ となり、G は巡回群となるから仮定に反する。

＊ $i=2$ とすると、$b^2=a^2$

$(b^2)^3=(a^2)^3=a^6=e$ より、$b^6=e$

$bab^{-1}=a^j$ とおくと、$a=b^6ab^{-6}=a^{j^6}$ が成り立つから、

$a=a^{j^6}\Longrightarrow j^6=1(\mathrm{mod}\,6)$

これを満たす j は 1 または 5 であるが $j=1$ のときは G は可換となるから、$j\neq 1$. よって、$j=5$ となる。（下表参照）

j	1	2	3	4	5
j^6	1	64	729	4096	15625
$\mathrm{mod}\,6$	1	4	3	4	1

以上より、$bab^{-1}=a^5$ を得た。

整理すると、$a^6=e, b^2=a^2, bab^{-1}=a^5$

このとき、$b^4=a^4$

ところが、$a^4=a^4a^6=a^{10}=(a^5)^2=(bab^{-1})^2=ba^2b^{-1}$

$(a^4)^2=(ba^2b^{-1})^2=ba^4b^{-1}=bb^4b^{-1}=b^4$

$\shortparallel$

$a^8=a^2$

よって、$b^4=a^2$ が成り立つから、$a^4=a^2\Longrightarrow a^2=e$ となり、$a^6=e$ に反する。

よって、$i\neq 2$

＊ $i=4$ のときも、$i=2$ のときと同じ議論が成立するから、$i\neq 4$

以上より、$i\neq 1,2,4,5$ となるから、$i=3$ となる。

＊ $i=3$ のとき、$bab^{-1}=a^j$ となる j を求めよう。

$b^2=a^3, (b^2)^2=(a^3)^2=a^6=e$ よって、$b^4=e$

$a=b^4ab^{-4}=a^{j^4}$ 、$a=a^{j^4}$ より、

$j^4=1(\mathrm{mod}\,6)$

これを満たす j は下表より、$j=5(j=1$ のときは可換となる）

j	1	2	3	4	5
j^4	1	16	81	256	625
$\mathrm{mod}\,6$	1	4	3	4	1

以上より、$bab^{-1}=a^5$ が導かれた。まとめると、

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

これは、$G\simeq Q_{12}$(四元数群）となる。

(2) - 2. $k=4$ のとき

この場合、G は位数 12 の**交代群** $\mathbf{A}_4$（偶置換からなる対称群の部分群）に同型 となる。証明はやや複雑なので省略する。

以上をまとめると、位数 12 の群は、

$G\simeq C_4\times C_3\simeq C_{12},\quad G\simeq C_2\times C_2\times C_3\simeq C_2\times C_6$

2 面体群 D_{12}, 四元数群 Q_{12}, 交代群 A_4

の５種類からなる。

＊本稿の執筆では、以下を参考とした。

・代数系入門（松坂和夫、岩波書店）

・群論への 30 講（志賀浩二、朝倉書店）

・群論の基礎（永尾汎、朝倉書店）

・小さい群の分類（ネット上の論文、作者不詳）

＊群の類別はこの論文によっている。

・群論（鈴木通夫、岩波書店）

＊筆者経歴

東京大学理学部数学科を経て教育学部卒業。証券会社、外資系通信社で金融・資本市場の業務を経験。専門は、債券資本市場。主な著書・論文：『信用リスクを読む』（日本評論社）、『信用リスクとＭ＆Ａ』（同）、『世界金融危機と信用リスク』（同）、『鎮めの文化と資本市場』（ブルームバーグ）、『金融派生商品』

メール：sakurasaku9286@willcom.com