有限群の同型類と元の位数の分布：Conformal groups とその表現

本稿では、一般線型群の部分群として現れる有限群の構造、元の位数の分布、および「元の位数のリストが完全に一致するが互いに同型ではない群のペア（conformal groups）」について、完全な証明と具体例を交えて解説する。

1. $GL(3, \mathbb{F}_3)$ の Sylow 3部分群

定義 1: Sylow p部分群 (Sylow p-subgroup)
G を有限群、p を素数とする。$|G| = p^n m$ （ただし p と m は互いに素）であるとき、位数が p^n である G の部分群を Sylow p部分群 と呼ぶ。Sylowの定理により、このような部分群は必ず存在する。

一般線型群 $G = GL(3, \mathbb{F}_3)$ の位数は以下のように計算される。

$$|G| = (3^3 - 1)(3^3 - 3)(3^3 - 3^2) = 26 \times 24 \times 18 = 11232 = 2^5 \cdot 3^3 \cdot 13$$

したがって、Sylow 3部分群 P の位数は $3^3 = 27$ である。一般に、$GL(n, \mathbb{F}_p)$ の Sylow p部分群は、対角成分がすべて 1 の上三角行列（単上三角行列）からなる群として実現できる。よって P は以下の形で表される行列からなる群である。

$$P = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{F}_3 \right\}$$

定義 2: Heisenberg群と超特殊p群 (extra-special p-group)
上記の行列表現を持つ群は $\mathbb{F}_3$ 上の Heisenberg群 と呼ばれる。これは非可換群である。さらに、中心 $Z(P)$ の位数が p であり、商群 $P/Z(P)$ が基本Abel群 (elementary abelian group) となるような p群を 超特殊p群 と呼ぶ。P はべき数 (exponent) が 3 の超特殊3群に該当する。

命題 1
群 P の任意の単位元以外の元の位数は 3 である。したがって P の元の位数のリストは「位数 1 が 1 個、位数 3 が 26 個」となる。

証明:
P の任意の元 A は、単位行列 I と狭義上三角行列 N を用いて $A = I + N$ と一意に表せる。ここで N は以下のように書ける。

$$N = \begin{pmatrix} 0 & a & c \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix}$$

行列の積を計算すると、N の冪乗は以下のようになる。

$$N^2 = \begin{pmatrix} 0 & 0 & ab \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad N^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0$$

I と N は可換 ($IN = NI = N$) であるため、二項定理を用いて A^3 を展開できる。

$$A^3 = (I+N)^3 = I + 3N + 3N^2 + N^3$$

係数の体は $\mathbb{F}_3$ （標数 3）であるため、$3 \equiv 0 \pmod 3$ となる。さらに $N^3 = 0$ であるため、次が成り立つ。

$$A^3 = I + 0 \cdot N + 0 \cdot N^2 + 0 = I$$

以上より、単位元以外のすべての元は 3 乗すると初めて単位元になる。□

2. Conformal groups の具体例

元の位数のリスト（各位数を持つ元の個数）が完全に一致するにもかかわらず、互いに同型ではない群のペアは conformal groups と呼ばれる。有限Abel群においては「元の位数のリストが一致すれば同型である」という定理が成り立つため、このようなペアを見つける場合、少なくとも一方は非可換群でなければならない。

2.1. 位数 27 のペア

先の群 P と位数の構成が全く同じ群として、基本Abel3群 $H = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ が挙げられる。H の単位元 $(0,0,0)$ 以外の任意の元 (x,y,z) を 3 倍（加法表記）すると $(3x,3y,3z) = (0,0,0)$ となるため、元の位数のリストは P と全く同じである。しかし H は可換、P は非可換であるため同型ではない。

2.2. 直積を用いた構成（位数 96 のペア）

既知の conformal groups のペアに、同じ群を直積で結合させることで、新たな非可換群のペアを構築できる。

> **例 1: 位数 96 のペア**
> 群 A: $(\mathbb{Z}_4 \times \mathbb{Z}_4) \times S_3$
> 群 B: $(\mathbb{Z}_2 \times Q_8) \times S_3$
> ここで S_3 は位数 6 の対称群、Q_8 は位数 8 の四元数群である。これらはともに非可換であり、元の位数のリストが一致するが、同型ではない。

証明 (同型ではないこと):
直積群の中心 (center) は各成分の中心の直積に同型である。すなわち $Z(X \times Y) \cong Z(X) \times Z(Y)$ が成り立つ。
S_3 の中心は単位元のみであるため、その位数は 1 である。
$\mathbb{Z}_4 \times \mathbb{Z}_4$ はAbel群であるから、中心は群全体に一致し、位数は 16 である。したがって群 A の中心の位数は $16 \times 1 = 16$ となる。
一方、$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ において中心は $\{\pm 1\}$ であり位数は 2 である。$\mathbb{Z}_2$ はAbel群であるから、$Z(\mathbb{Z}_2 \times Q_8) \cong \mathbb{Z}_2 \times Z(Q_8)$ となり、位数は $2 \times 2 = 4$ である。したがって群 B の中心の位数は $4 \times 1 = 4$ となる。
中心の位数が異なるため、群 A と群 B は同型ではない。□

2.3. 位数 16 の最小のペア

元の位数のリストが等しく、互いに同型ではない群のペアは、位数が 15 以下の群には存在しない。最小の例は位数 16 である。

例 2: 位数 16 のペア
群 A: $Q_8 \times \mathbb{Z}_2$
群 B: $\mathbb{Z}_4 \rtimes \mathbb{Z}_4$
（群 B は生成元 a, b を持ち、関係式 $a^4 = 1, b^4 = 1, bab^{-1} = a^{-1}$ で定義される半直積 (semi-direct product) である）

元の位数	群 A の元の個数	群 B の元の個数
1	1	1
2	3	3
4	12	12

定理 1
群 A と群 B は元の位数のリストが等しく、かつ互いに同型ではない非可換群である。

証明:
両群とも中心の位数は 4 であるため、中心の位数では区別できない。「ある元の平方 (square) として表される元の集合」を調べる。

群 A の場合: 任意の元は $(q, n) \in Q_8 \times \mathbb{Z}_2$ と表される（$\mathbb{Z}_2$ を乗法群 $\{1, z\}$ とみなし、$z^2 = 1$ とする）。この元の平方は (q^2, n^2) である。Q_8 の任意の元の平方は 1 または -1 であり、$n^2 = 1$ であるから、平方として現れる元は $(1, 1)$ または $(-1, 1)$ のみである。このうち、位数 2 の元は $(-1, 1)$ の 1 個だけである。

群 B の場合: 任意の元は $a^i b^j$ （$0 \le i, j \le 3$）の形で書ける。関係式 $ba = a^{-1}b = a^3 b$ を用いて平方元を計算する。

- $j = 0$ のとき: $(a^i)^2 = a^{2i} \in \{1, a^2\}$。
- $j = 1$ のとき: $(a^i b)^2 = a^i b a^i b = a^i a^{-i} b^2 = b^2$。
- $j = 2$ のとき: $b^2 a = b(a^{-1} b) = ab^2$ より b^2 は a と可換である。したがって $(a^i b^2)^2 = a^{2i} b^4 = a^{2i} \in \{1, a^2\}$。
- $j = 3$ のとき: $b^3 a = b^2 a^{-1} b = a^{-1} b^3$ より、$(a^i b^3)^2 = a^i a^{-i} b^6 = b^2$。

したがって、平方として現れる元は $\{1, a^2, b^2\}$ の 3 種類のみである。このうち、a^2 と b^2 はいずれも位数 2 の元である。すなわち、平方元の中に位数 2 の元が 2 個存在する。

構造的性質（平方元の集合における位数 2 の元の個数）が異なるため、群 A と群 B は同型ではない。□

3. 部分群としての実現と行列表現

群 A と群 B はそれぞれ異なる背景から様々な空間の部分群として実現できる。これを調べることで群の内部構造が浮き彫りになる。

3.1. 対称群への埋め込み

Cayleyの定理により、位数 16 の群は対称群 S_{16} に埋め込めるが、より小さな対称群に埋め込めるかは群作用の性質に依存する。

> **命題 2**
> 群 B ($\mathbb{Z}_4 \rtimes \mathbb{Z}_4$) は対称群 S_8 の部分群として実現できるが、群 A ($Q_8 \times \mathbb{Z}_2$) は S_8 の部分群として実現できず、最小でも S_{12} を必要とする。

証明:
群を対称群に埋め込むことは、共通部分が自明 (すなわち $\{1\}$) になるような部分群たちの集合を見つけ、それらによる剰余類の置換表現を構成することと同値である。

群 B の場合: 位数 4 の部分群 $H_1 = \langle a \rangle$ と $H_2 = \langle b \rangle$ を考える。それぞれの指数は $16/4 = 4$ である。H_1 と H_2 に群を左から作用させるとき、その作用の核 (kernel) はそれぞれ $\langle a \rangle$ と $\langle b^2 \rangle$ となる。これらの共通部分は $\langle a \rangle \cap \langle b^2 \rangle = \{1\}$ であるため、この2つの軌道（合計 $4+4=8$ 点）への作用は忠実である。したがって S_8 に埋め込める。

群 A の場合: 群 A の位数 4 以上のすべての部分群は、位数 2 の元 $(-1, 1)$ を必ず含んでしまう。すなわち、指数 4 以下（軌道の長さが 4 以下）の表現のみを集めても、$(-1, 1)$ の作用が自明となってしまい忠実な表現を得られない。これを回避するには $(-1, 1)$ を含まない部分群による作用が必要となる。そのような最大の群は $K = \langle (1, -1) \rangle$ (位数 2) である。この部分群の指数は 8 であり、8 点の軌道を要する。しかしこれだけでは $(1, -1)$ の作用が自明になるため、これを補うために指数 4 の軌道を追加する必要がある。したがって最小の点の数は $8+4=12$ となり、S_8 には埋め込めない。□

3.2. 有限体上の行列表現

これらの群を $GL(n, \mathbb{F}_p)$ の部分群として実現する問題を考える。

$GL(3, \mathbb{F}_5)$ における実現:
$n=2$ では群 A の中心 $\mathbb{Z}_2 \times \mathbb{Z}_2$ を表現できないため不可能である。また、$n=3$ の場合、$p=2,3$ では群 B の関係式によって情報が潰れてしまう。条件を満たす最小の組み合わせは $GL(3, \mathbb{F}_5)$ である。ここで $4 \equiv -1 \pmod 5$ に注意する。

群 B の生成元 a, b は以下のように実現される。

$$a = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

これにより $bab^{-1} = a^{-1}$ を満たしつつ、$b^2 \equiv \mathrm{diag}(1,1,4) \equiv \mathrm{diag}(1,1,-1) \pmod 5$ となるため、$b^2 \neq a^2$ が保たれる。

$GL(5, \mathbb{F}_2)$ における実現:

標数 2 の世界（すなわち $\mathbb{F}_2$）では、位数 4 の行列の挙動が強く制約される。$n=4$ では、余白が足りず情報が縮退してしまうため、群 A ($Q_8 \times \mathbb{Z}_2$) および群 B ($\mathbb{Z}_4 \rtimes \mathbb{Z}_4$) ともに忠実な表現を持たない。次元を $n=5$ に拡張することで、初めて両者を部分群として埋め込むことができる。

群 B ($\mathbb{Z}_4 \rtimes \mathbb{Z}_4$) の実現:

群 B の $\mathbb{F}_2$ 上の生成元行列 M_a, M_b は以下の通りに構成できる。これはシロー2部分群の中に美しく収まる。

$$M_a = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad M_b = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

行列の積を $\mathbb{F}_2$ 上で計算することで、$M_a^4 = I, M_b^4 = I$ および $M_b M_a M_b^{-1} = M_a^{-1}$ (M_a^3 に等しい) が成り立つことが確認できる。

群 A ($Q_8 \times \mathbb{Z}_2$) の実現:

四元数群 Q_8 を標数 2 の体 $\mathbb{F}_2$ 上で忠実に表現するためには、唯一の位数 2 の元 (-1) が「$-I = I$」となって情報が潰れてしまわないよう、慎重に 4 次元の不変部分空間を切り出す必要がある。生成元 i, j に対応する 4×4 の忠実な行列表現を $M_i, M_j \in GL(4, \mathbb{F}_2)$ とおく。これらは $M_i^2 = M_j^2 \neq I$ かつ $M_i M_j = M_j M_i^3$ を満たす。
これらを 5×5 のブロック対角行列に拡張し、右下の成分に 1 を配置する（$\mathbf{0}$ は 4×1 の零ベクトルを表す）。

$$A_i = \begin{pmatrix} M_i & \mathbf{0} \\ \mathbf{0}^T & 1 \end{pmatrix}, \quad A_j = \begin{pmatrix} M_j & \mathbf{0} \\ \mathbf{0}^T & 1 \end{pmatrix}$$

次に、独立した $\mathbb{Z}_2$ 成分を組み込む。M_i, M_j がベクトル $(1,0,0,0)^T$ を固定するように基底を取り直したとすると、$\mathbb{Z}_2$ の生成元となる行列 A_z を次のように構成できる。

$$A_z = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A_z は $A_z^2 = I$ を満たす位数 2 の行列であり、第 5 成分から第 1 成分への寄与のみを持つ。A_i, A_j は第 1 成分を固定するため、A_z は A_i, A_j の両方と完全に可換になる。この構成により、$Q_8 \times \mathbb{Z}_2$ のすべての元が潰れることなく $GL(5, \mathbb{F}_2)$ の部分群として実現される。

4. 代表的な非可換群の定義と表示

次章の分類表に現れる p群（特に位数8および16の非可換群）について、生成元と基本関係式（presentation）を用いた厳密な定義を以下にまとめる。群の構造を明示するため、それぞれの関係式がどのように群の演算を支配しているかに注目されたい。

> **Q_8：四元数群 (Quaternion group)**
> 位数は 8。生成元 i, j を用いて以下のように定義される。

$$Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, jij^{-1} = i^{-1} \rangle$$

これは $\{\pm 1, \pm i, \pm j, \pm k\}$ として知られる表現と同値であり、特有の性質として「すべての部分群が正規部分群となる非可換群（ハミルトン群）」の最小の例である。

Q_{16}：一般四元数群 (Generalized quaternion group)
位数は 16。Q_8 を自然に拡張したものであり、以下で定義される。

$$Q_{16} = \langle a, b \mid a^8 = 1, b^2 = a^4, bab^{-1} = a^{-1} \rangle$$

位数 8 の巡回部分群 $\langle a \rangle$ を持ち、元の平方がこの巡回部分群の中心元の平方元（すなわち a^4）に一致する。

M_{16}：モジュラー群 (Modular maximal-cyclic group)
位数は 16。位数 8 の巡回部分群 $\langle a \rangle$ を持ち、もう1つの生成元 b の作用がモジュラー演算に似た性質を持つ。

$$M_{16} = \langle a, b \mid a^8 = 1, b^2 = 1, bab^{-1} = a^5 \rangle$$

ここで、a の指数「5」は $16/2 + 1 = 9$ が $\pmod 8$ で 1 になる性質（より一般に $2^{n-1} + 1$）に由来する。

SD_{16}：準二面体群 (Semidihedral group / Quasidihedral group)
位数は 16。二面体群と似ているが、元の反転作用がわずかにずれている。

$$SD_{16} = \langle a, b \mid a^8 = 1, b^2 = 1, bab^{-1} = a^3 \rangle$$

ここで、a の指数「3」は $16/2 - 1 = 7$ ではなく、$2^{n-2} - 1$ に由来する（位数が 2^n の場合）。二面体群の反転作用 $a^{-1} = a^7$ とは異なる構造を持つ。

$D_8 * \mathbb{Z}_4$：中心積 (Central product)
位数は 16。位数 8 の二面体群 D_8 と位数 4 の巡回群 $\mathbb{Z}_4$ の直積を構成し、それぞれの中心部分群を同一視（融合）して得られる群である。
$D_8 = \langle r, s \mid r^4 = 1, s^2 = 1, srs = r^{-1} \rangle$ の中心は $Z(D_8) = \langle r^2 \rangle$ であり、$\mathbb{Z}_4 = \langle c \mid c^4 = 1 \rangle$ の唯一の位数 2 の部分群は $\langle c^2 \rangle$ である。これらを $r^2 = c^2$ として結合させる。

$$D_8 * \mathbb{Z}_4 = \langle r, s, c \mid r^4 = 1, s^2 = 1, srs = r^{-1}, c^4 = 1, rc = cr, sc = cs, r^2 = c^2 \rangle$$

5. 低位数の群の分類と元の位数の分布

同型ではないが元の位数の分布が一致する群（conformal groups）の存在をより体系的に理解するため、位数が小さな素数べきの群（位数 8, 9, 16, 27, 81）の分類と、それぞれにおける「各位数を持つ元の個数」のリストを整理する。

5.1. 位数 8 の群（全 5 種）

元の位数の分布 (位数: 1, 2, 4, 8)	同型類の数	該当する群の構造

$1, 1, 2, 4$	1種	$\mathbb{Z}_8$ (可換)
$1, 3, 4, 0$	1種	$\mathbb{Z}_4 \times \mathbb{Z}_2$ (可換)
$1, 7, 0, 0$	1種	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (可換)
$1, 5, 2, 0$	1種	D_8 (二面体群, 非可換)
$1, 1, 6, 0$	1種	Q_8 (四元数群, 非可換)

5.2. 位数 9 の群（全 2 種）

元の位数の分布 (位数: 1, 3, 9)	同型類の数	該当する群の構造
$1, 2, 6$	1種	$\mathbb{Z}_9$ (可換)
$1, 8, 0$	1種	$\mathbb{Z}_3 \times \mathbb{Z}_3$ (可換)

5.3. 位数 16 の群（全 14 種）

元の位数の分布 (位数: 1, 2, 4, 8, 16)	同型類の数	該当する群の構造
$1, 1, 2, 4, 8$	1種	$\mathbb{Z}_{16}$ (可換)
$1, 3, 4, 8, 0$	2種	$\mathbb{Z}_8 \times \mathbb{Z}_2$ (可換) M_{16} (Modular群, 非可換)
$1, 3, 12, 0, 0$	4種	$\mathbb{Z}_4 \times \mathbb{Z}_4$ (可換) $Q_8 \times \mathbb{Z}_2$ (非可換, 本稿の群A) $\mathbb{Z}_4 \rtimes \mathbb{Z}_4$ (非可換, 本稿の群B) $D_8 * \mathbb{Z}_4$ (中心積, 非可換)
$1, 7, 8, 0, 0$	2種	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (可換) $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_4$ (非可換)
$1, 15, 0, 0, 0$	1種	$\mathbb{Z}_2^4$ (可換)
$1, 9, 2, 4, 0$	1種	D_{16} (二面体群, 非可換)
$1, 1, 10, 4, 0$	1種	Q_{16} (一般四元数群, 非可換)
$1, 5, 6, 4, 0$	1種	SD_{16} (準二面体群 / Semi-dihedral, 非可換)
$1, 11, 4, 0, 0$	1種	$D_8 \times \mathbb{Z}_2$ (非可換)

5.4. 位数 27 の群（全 5 種）

元の位数の分布 (位数: 1, 3, 9, 27)	同型類の数	該当する群の構造
1, 2, 6, 18	1種	$\mathbb{Z}_{27}$ (可換)
1, 8, 18, 0	2種	$\mathbb{Z}_9 \times \mathbb{Z}_3$ (可換) M_{27} (べき数9の超特殊3群, 非可換)
1, 26, 0, 0	2種	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ (可換) P (べき数3のHeisenberg群, 非可換, 本稿1章の群)

5.5. 位数 81 の群（全 15 種）

元の位数の分布 (位数: 1, 3, 9, 27, 81)	同型類の数	該当する群の構造
1, 2, 6, 18, 54	1種	$\mathbb{Z}_{81}$ (可換)
1, 8, 18, 54, 0	2種	$\mathbb{Z}_{27} \times \mathbb{Z}_3$ (可換) 他 1種 (非可換)
1, 8, 72, 0, 0	2種	$\mathbb{Z}_9 \times \mathbb{Z}_9$ (可換) 他 1種 (非可換)
1, 26, 54, 0, 0	7種	$\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ (可換) 他 6種 (非可換)
1, 80, 0, 0, 0	3種	$\mathbb{Z}_3^4$ (可換) 他 2種 (非可換)

6. 参考文献

本稿で解説した群論の基礎概念、Sylowの定理、超特殊p群、および表現論の詳細は、以下の標準的文献にて深く学ぶことができる。

- Dummit, D. S., & Foote, R. M. (2004). *Abstract Algebra* (3rd ed.). John Wiley & Sons.
  URL: https://archive.org/details/abstractalgebra0000dumm_u7a5
- Gorenstein, D. (1980). *Finite Groups* (2nd ed.). Chelsea Publishing Company.
  URL: https://archive.org/details/finitegroups0000gore
- Suzuki, M. (1982). *Group Theory I*. Springer-Verlag.
  URL: https://link.springer.com/book/10.1007/978-3-642-61841-8