現象数理研究 IV 卒業研究レポート

ルービックキューブと群論

明治大学 総合数理学部 現象数理学科
学籍番号：2610210048
大羽 志龍

2025 年 3 月 2 日

目 次

記号一覧

ここに載せたもの以外で新しく定義する記号は本文中で詳しく説明する.

$A \coloneqq B$: A を B で定義する.

$\exists!$: $\exists! a, \sim \ \Leftrightarrow a$ が一意に存在して〜.

$\mathbb{N}$: 自然数全体の集合 $\mathbb{N} \coloneqq \{1, 2, \dots\}$.

$A \setminus B$: 集合 A, B の差集合 $A \setminus B \coloneqq \{x \mid x \in A \wedge x \notin B\}$.

$|A|$: 集合 A の濃度 $|A|$.

A^n : 集合 A の n 個の直積 $A^n \coloneqq \{(a_1, a_2, \dots, a_n) \mid a_1, a_2, \dots, a_n \in A\}$.

$f(A)$: 写像 $f : X \to Y$ による $A \subset X$ の像 $f(A) \coloneqq \{f(x) \in Y \mid x \in A\}$.

$f|_A$: 写像 $f : X \to Y$ の $A \subset X$ への制限 $f|_A : A \to Y;\ x \mapsto f(x)$.

gf : 写像 $f : X \to Y,\ g : Y \to Z$ の合成 $gf : X \to Z;\ x \mapsto g(f(x))$. 本稿では積と呼ぶ.

f^n, f^0, f^{-n} : 写像 $f : X \to X$ の冪 $f^n \coloneqq \underbrace{ff \cdots f}_{n},\ f^0(x) \coloneqq x\ (x \in X),\ f^{-n} \coloneqq \underbrace{f^{-1}f^{-1} \cdots f^{-1}}_{n}$.

$\mathrm{Map}(A, B)$: 配置集合 $\mathrm{Map}(A, B) \coloneqq \{f \mid f : A \to B\}$.

$-g, g^{-1}$: 群の加法逆元 $-g$, 乗法逆元 g^{-1}.

I_n : $I_n \coloneqq \{1, 2, \dots, n\}$.

S_n : n 次対称群 $S_n \coloneqq \{\sigma : I_n \to I_n \mid \sigma$ は全単射 $\}$.

ε : 恒等置換 $\varepsilon \in S_n$.

o_n : 長さ n の巡回置換 $o_n \coloneqq (1\ 2\ \cdots\ n) \in S_n$.

sgn : 符号関数 $\mathrm{sgn} : S_n \to \{-1, 1\}$;

$$\sigma \mapsto \mathrm{sgn}(\sigma) \coloneqq \begin{cases} 1 & (\sigma \text{ は偶置換}) \\ -1 & (\sigma \text{ は奇置換}) \end{cases}.$$

$\mathrm{supp}(\sigma)$: 置換 $\sigma \in S_n$ の台 $\mathrm{supp}(\sigma) \coloneqq \{i \in I_n \mid \sigma(i) \neq i\}$.

$\mathbb{Z}_n$: n を法とする加法による剰余群 $\mathbb{Z}_n \coloneqq \{0, 1, \dots, n-1\}$. 演算記号は $+$ を用いるが, $\mathbb{Z}_n$ の元に対する演算は全て n を法とする加法とみなす.

$\mathbf{0}_n$: $\mathbf{0}_n \coloneqq \underbrace{(0, 0, \dots, 0)}_{n}$.

gS : 群 G の元 g とその部分集合 S に対して, $gS \coloneqq \{gs \mid s \in S\}$.

$G \cong H$: 群 G, H は同型である.

$\mathrm{Aut}(G)$: 群 G の自己同型群 $\mathrm{Aut}(G) \coloneqq \{f : G \to G \mid f$ は同型 $\}$.

$[g, h]$: 群 G の元 g, h の交換子 $[g, h] \coloneqq h^{-1}g^{-1}hg$.

G^{op} : 群 $G = (G, *)$ に対して, $g_1 *' g_2 \coloneqq g_2 * g_1\ (g_1, g_2 \in G)$ を演算とする群 G の逆群 $G^{\mathrm{op}} \coloneqq (G, *')$.

1　はじめに

私は高校生の頃からルービックキューブの早解きを趣味としており, ルービックキューブの数学的性質にも興味を持っていたので, この機会に詳しく学習してみることにした. 本レポートは、群論を用いてルービックキューブの数学的性質の基本事項を明らかにすることを主題に置いている. より具体的には, ルービックキューブの模様のパターンの総数を求めることを最終目標とし, そこに至るまでの内容の大筋を Joyner[1] を参考にしてまとめた.

本稿では厳密さと直感のギャップを埋めるために私が導入した, [1] に登場しない定義がいくつか登場する (定義 3.2 など). また, 前提となる群論に関する知識は付録にまとめた.

2　ルービックキューブについて

2.1　操作の定義

ルービックキューブとは, 各面が異なる色で塗られかつ各面が 3×3 分割された立方体のパズルである. ルービックキューブにおいて, 各面を構成する計 26 個の立方体を**小方体**と呼び, 各小方体の見えている面のことを**小面**と呼ぶ. また, ルービックキューブを手に持ち, 上下の面と左右の面の区別がつくようにある面を正面から見たとき, 右面を **R 面**, 左面を **L 面**, 上面を **U 面**, 下面を **D 面**, 前面を **F 面**, 後面を **B 面**と呼ぶ[*1](図 2.1). これらの 6 つの表記を**シングマスター記法**という.

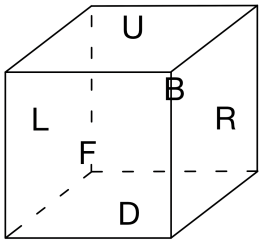

図 2.1 各面に対応する記号

ここで, **ルービックキューブの規則に従った操作** (あるいは単に**操作**) とは, 以下のように定義される動作のことである：

(1) 図 2.2 の x, y, z 軸いずれかのまわりに動く 1 層, あるいは同じ軸に対して動く 2, 3 層を一緒に $90m$ 度 (m は整数の定数) 回転する動作は, 1 回の操作である.

(2) n 回の操作の後に 1 回の操作をする動作は, $n+1$ 回の操作である ($n \in \mathbb{N}$).

(3) 以上の手続きでできる n 回の操作のことを操作と呼ぶ.

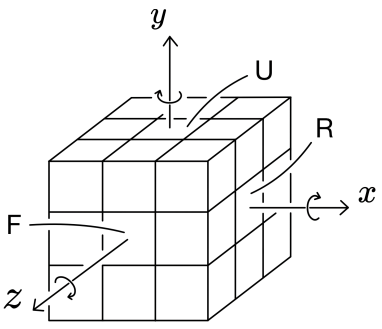

図 2.2 各面に対応する軸

ただし, 各軸の負方向に右ねじが進む方向を回転の正方向とする. さらに, 操作によってシングマスター記法を振り分ける位置や図 2.2 の軸は移動せず, 空間に固定されているものとする. 特に, 同じ軸に対して動く 3 層の回転のみからなる操作のことを**ルービックキューブの持ち替え**という.

[*1] それぞれ Right, Left, Up, Down, Front, Back の頭文字から取っている.

このとき, いくつかの操作に以下のように名前をつける：

- 各層の回転：

  R　R 面を正面から見て時計まわりに 90 度回転する.

  L　L 面を正面から見て時計まわりに 90 度回転する.

  U　U 面を正面から見て時計まわりに 90 度回転する.

  D　D 面を正面から見て時計まわりに 90 度回転する.

  F　F 面を正面から見て時計まわりに 90 度回転する.

  B　B 面を正面から見て時計まわりに 90 度回転する.

  M　x 軸まわりに動く中央の層を x 軸まわりに -90 度回転する.

  E　y 軸まわりに動く中央の層を y 軸まわりに -90 度回転する.

  S　z 軸まわりに動く中央の層を z 軸まわりに 90 度回転する.

- 持ち替え：

  x　ルービックキューブ全体を x 軸まわりに 90 度回転する.

  y　ルービックキューブ全体を y 軸まわりに 90 度回転する.

  z　ルービックキューブ全体を z 軸まわりに 90 度回転する.

M, E, S は特に**スライスムーブ**とも呼ばれ, それぞれ Middle, Equator, Standing の頭文字から取ったものである[*2].

2.2　基本操作

2 つのルービックキューブが**同じ配置**であるとは, 全ての小方体について図 2.2 の軸で定まる座標および面の向きが等しいときのことをいう. また, 2 つの操作が**同じ操作**であるとは, 配置が同じ 2 つのルービックキューブにそれぞれ操作をしたときに 2 つがまた同じ配置になるときのことをいう. このとき, 各層の回転操作はそれぞれ $R, L, U, D, F, B, M, E, S$ の何回かの繰り返しの操作と同じ操作となり, さらに

$$M \text{ は } R \text{ 1 回} \to L \text{ 3 回} \to x \text{ 3 回と同じ操作,}$$
$$E \text{ は } U \text{ 1 回} \to D \text{ 3 回} \to y \text{ 3 回と同じ操作,}$$
$$S \text{ は } F \text{ 3 回} \to B \text{ 1 回} \to z \text{ 1 回と同じ操作}$$

である. したがって, 2 つのルービックキューブが**同じ模様**であることを, 2 つのルービックキューブが同じ配置または持ち替えによって同じ配置になるときのこととして定義すると, 上記の事実よりルービックキューブの模様を変化させうる操作は

$$R, L, U, D, F, B$$

からなる操作のみである. これら 6 つの操作を**基本操作**と呼ぶ. 本稿では, ルービックキューブの“配置”ではなく“模様”について考察することにし, 今後は**基本操作からなる操作を全ての操作とみなして議論する**.

[*2] M, E については, 90 度回転ではなくなぜか -90 度回転とする定義が一般的となっている (例えば [2]).

3　操作と置換の同一視

3.1　キューブへの番号づけ

ルービックキューブの操作を数学的に解釈するために, ルービックキューブのいくつかの箇所に番号をつけよう (ここでは [1] を参考にする). まずは各小面に番号をつける. ただし, 各面の中央の小方体 (1 **面体**という) は基本操作によって移動しないので, その小面には各面のシングマスター記法に対応するアルファベットを明示的につけておく (図 3.1).

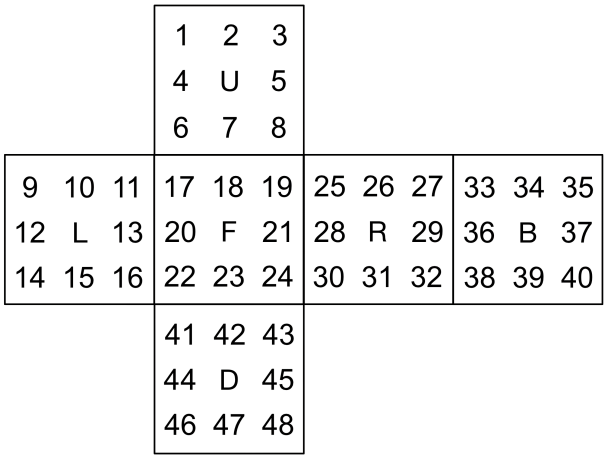

図 3.1 各小面に対応する番号

ここでこれらの番号をシングマスター記法などと同様に空間に固定されているものとすると, 操作を 48 次の置換と同一視することができ[*3], 2.2 節で定義した操作の相等は写像の相等とみなされる. 特に, 各基本操作は以下のような巡回置換の積となる：

$$
\begin{aligned}
R &= (3\ 38\ 43\ 19)(5\ 36\ 45\ 21)(8\ 33\ 48\ 24)(25\ 27\ 32\ 30)(26\ 29\ 31\ 28),\\
L &= (1\ 17\ 41\ 40)(4\ 20\ 44\ 37)(6\ 22\ 46\ 35)(9\ 11\ 16\ 14)(10\ 13\ 15\ 12),\\
U &= (1\ 3\ 8\ 6)(2\ 5\ 7\ 4)(9\ 33\ 25\ 17)(10\ 34\ 26\ 18)(11\ 35\ 27\ 19),\\
D &= (14\ 22\ 30\ 38)(15\ 23\ 31\ 39)(16\ 24\ 32\ 40)(41\ 43\ 48\ 46)(42\ 45\ 47\ 44),\\
F &= (6\ 25\ 43\ 16)(7\ 28\ 42\ 13)(8\ 30\ 41\ 11)(17\ 19\ 24\ 22)(18\ 21\ 23\ 20),\\
B &= (1\ 14\ 48\ 27)(2\ 12\ 47\ 29)(3\ 9\ 46\ 32)(33\ 35\ 40\ 38)(34\ 37\ 39\ 36).
\end{aligned}
$$

基本操作全体の集合には, $G_{\mathrm{b}} := \{R, L, U, D, F, B\}$ と名前をつけておく.

ここで, ルービックキューブの**頂点**とは, 小面を 3 つ持つ空間に固定された小方体のことを指す. 一方で, 小面を 3 つ持つ色のついた小方体 (すなわち, 操作によって動く小方体) のことを 3 **面体**という[*4]. 同様に, ルービックキューブの**辺**とは, 小面を 2 つ持つ空間に固定された小方体のことを指す. 一方で, 小面を 2 つ持つ色のついた小方体のことを 2 **面体**という.

さて, 図 3.1 と同様に頂点にも番号をつけ, さらに各頂点の 1 つの小面に $+$ 印をつける (図 3.2). このとき, i 番目の頂点を頂点 i, 頂点 i に位置する 3 面体を 3 面体 i と呼ぶ. さらに, 頂点 i と対応する図 3.1 におけるの 3 つの番号を元とする集合を C_i, 各頂点の $+$ 印のついた小面についている番号全体の集合を C_+ とし, C_{all} を C_i $(i \in I_8)$ の和集合とする：

[*3] n 回の操作は, 写像の n 回の合成とみなすこととなる.
[*4] 例えば, ある頂点に位置する 3 面体が別の頂点の位置に移動する, といったように表現する.

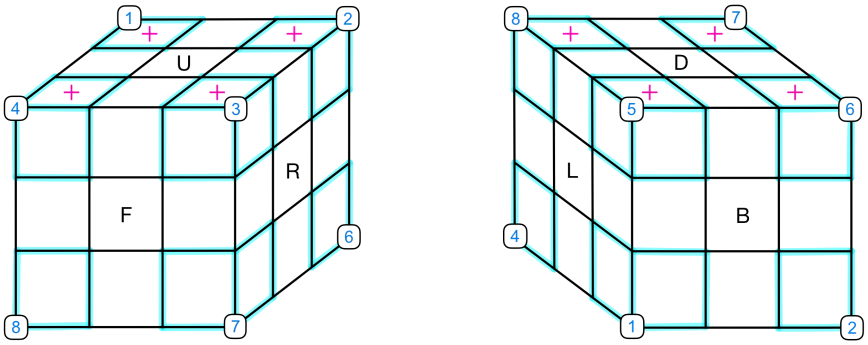

図 3.2 頂点の番号と印

$$C_1 := \{1, 9, 35\},\ C_2 := \{3, 27, 33\},\ C_3 := \{8, 19, 25\},\ C_4 := \{6, 11, 17\},$$
$$C_5 := \{14, 40, 46\},\ C_6 := \{32, 38, 48\},\ C_7 := \{24, 30, 43\},\ C_8 := \{16, 22, 41\},$$
$$C_+ := \{1, 3, 6, 8, 41, 43, 46, 48\},\ C_{\text{all}} := C_1 \cup C_2 \cup \cdots \cup C_8.$$

同様に, 辺にも番号をつけ, 各辺の 1 つの小面に + 印をつける (図 3.3). このとき, i 番目の辺を辺 i, 辺 i に位置する 2 面体を 2 面体 i と呼ぶ. さらに, 辺 i と対応する図 3.1 における 2 つの番号を元とする集合を E_i, 各辺の + 印のついた小面についている番号全体の集合を E_+ とし, E_{all} を E_i $(i \in I_{12})$ の和集合とする：

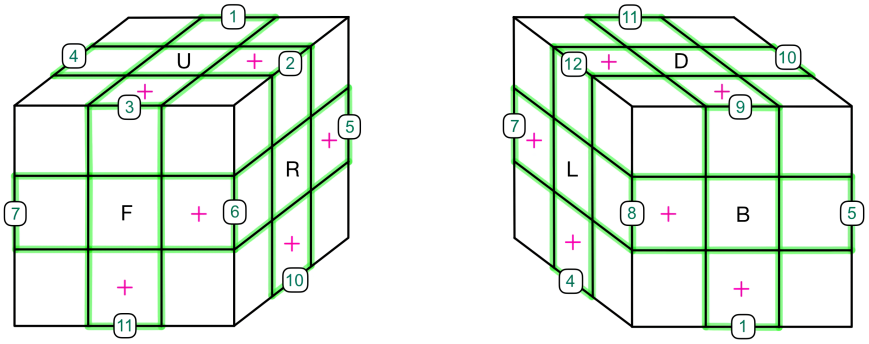

図 3.3 辺の番号と印

$$E_1 := \{2, 34\},\ E_2 := \{5, 26\},\ E_3 := \{7, 18\},\ E_4 := \{4, 10\},$$
$$E_5 := \{29, 36\},\ E_6 := \{21, 28\},\ E_7 := \{13, 20\},\ E_8 := \{12, 37\},$$
$$E_9 := \{39, 47\},\ E_{10} := \{31, 45\},\ E_{11} := \{23, 42\},\ E_{12} := \{15, 44\},$$
$$E_+ := \{5, 7, 10, 13, 21, 23, 29, 31, 34, 37, 44, 47\},\ E_{\text{all}} := E_1 \cup E_2 \cup \cdots \cup E_{12}.$$

3.2 小方体の移動

まず, 頂点および辺の向きを定めるために, 各小面の番号に名前をつける.

定義 3.1 $k \in I_3,\ i \in I_8$ に対し $c(k, i) \in C_{\text{all}}$ を, $c(1, i) \in C_i \cap C_+,\ c(2, i), c(3, i) \in C_i \setminus C_+$ であって, k の順番が頂点 i の小面に対する時計回りの順番に対応するものとして定める. また, $k' \in I_2,\ i' \in I_{12}$ に対し $e(k', i') \in E_{\text{all}}$ を, $e(1, i') \in E_{i'} \cap E_+,\ e(2, i') \in E_{i'} \setminus E_+$ を満たすものとして定める (図 3.4). ◇

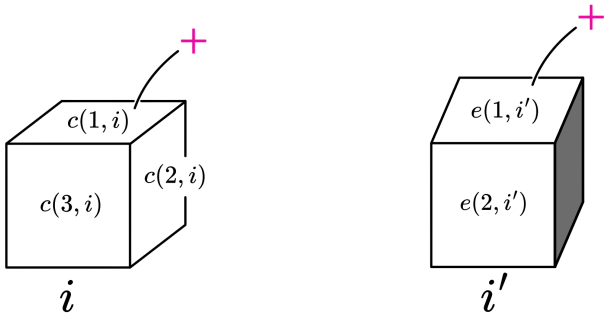

図 3.4 頂点 i, 辺 i' における小面の番号

ここで, 3 面体の移動を定義しよう.

定義 3.2 $g \in S_{48},\ i, j \in I_8$ とする. $g : C_i \rightsquigarrow C_j$ であることを, ある $n \in \mathbb{Z}_3$ が存在して, 任意の $k \in I_3$ について $g(c(k, i)) = c({o_3}^n(k), j)$ となるときのこととして定義する. このとき, n のことを**回転量**と呼び, 「g **により 3 面体** i **は回転量** n **で頂点** j **に移動した**」などという. $\diamond$

言い換えると, $g : C_i \rightsquigarrow C_j$ とは, 置換 g によって 3 面体 i が**小面を貼り替えないまま**頂点 j に移動するときのことを表したもので, 単なる集合の相等 $g(C_i) = C_j$ よりも元の対応を縛るものである[*5]. ゆえに, 以下の系が従う.

系 3.1 $\forall g \in S_{48}, \forall i, j \in I_8, (g : C_i \rightsquigarrow C_j \ \Rightarrow\ g(C_i) = C_j)$. $\diamond$

証明 任意に $g \in S_{48}$ および $i, j \in I_8$ をとる. $g : C_i \rightsquigarrow C_j$ とすると, 定義 3.2 より, ある $n \in \mathbb{Z}_3$ が存在して $g(C_i) = \{c({o_3}^n(k), j) \mid k \in I_3\} = \{c(l, j) \mid l \in I_3\} = C_j$. ■

また, 回転量の一意性も示しておく.

命題 3.1 $\forall i \in I_8, \forall n_1, n_2 \in \mathbb{Z}_3, ((\forall k \in I_3, c({o_3}^{n_1}(k), i) = c({o_3}^{n_2}(k), i)) \ \Rightarrow\ n_1 = n_2)$. $\diamond$

証明 任意に $i \in I_8$ および $n_1, n_2 \in \mathbb{Z}_3$ をとる. $c({o_3}^{n_1}(k), i) = c({o_3}^{n_2}(k), i)\ (k \in I_3)$ のとき, ${o_3}^{n_1} = {o_3}^{n_2}$ となるが, ${o_3}^0, {o_3}^1, {o_3}^2$ は全て相異なる写像なので, $n_1 = n_2$ である. ■

さらに, 以下の命題も重要である.

命題 3.2 任意の $i, j, k \in I_8,\ g, h \in S_{48}$ について, 以下の (1)〜(3) が成り立つ:

(1) $\varepsilon : C_i \rightsquigarrow C_i$.

(2) $g : C_i \rightsquigarrow C_j \ \Rightarrow\ g^{-1} : C_j \rightsquigarrow C_i$.

(3) $(g : C_i \rightsquigarrow C_j,\ h : C_j \rightsquigarrow C_k) \ \Rightarrow\ hg : C_i \rightsquigarrow C_k$. $\diamond$

証明
任意に $i, j, k \in I_8$ および $g, h \in S_{48}$ をとる.

(1) $\varepsilon(c(l, i)) = c(l, i) = c({o_3}^0(l), i)\ (l \in I_3)$ より, $\varepsilon : C_i \rightsquigarrow C_i$.

(2) $g : C_i \rightsquigarrow C_j$ とすると, ある $n \in \mathbb{Z}_3$ が存在して $g(c(l, i)) = c({o_3}^n(l), j)\ (l \in I_3)$ となる. ゆえに $g^{-1}(c(l, j)) = c({o_3}^{-n}(l), i)\ (l \in I_3)$ であり, $-n \in \mathbb{Z}_3$ から $g^{-1} : C_j \rightsquigarrow C_i$ が従う.

(3) まず, $g : C_i \rightsquigarrow C_j$ とすると, ある $n_1 \in \mathbb{Z}_3$ が存在して $g(c(l, i)) = c({o_3}^{n_1}(l), j)\ (l \in I_3)$ となる. 一方で, $h : C_j \rightsquigarrow C_k$ でもあるから, $h(c({o_3}^{n_1}(l), j)) = c({o_3}^{n_2}({o_3}^{n_1}(l)), k)\ (l \in I_3)$ なる $n_2 \in \mathbb{Z}_3$ がとれる. このとき, $hg(c(l, i)) = c({o_3}^{n_1+n_2}(l), k)\ (l \in I_3)$ であり, $n_1 + n_2 \in \mathbb{Z}_3$ より $hg : C_i \rightsquigarrow C_k$ が従う. ■

[*5] $g(C_i) = C_j$ では 3 つの小面に対応する元の順番までは指定できないため, 小面を貼り替えない移動を表すことはできない.

さらに, 定義 3.2 と同様にして, 2 面体の移動を定義しよう.

定義 3.3 $g \in S_{48},\ i, j \in I_{12}$ とする. $g : E_i \rightsquigarrow E_j$ であることを, ある $m \in \mathbb{Z}_2$ が存在して, 任意の $k \in I_2$ について $g(e(k, i)) = e(o_2{}^m(k), j)$ となるときのこととして定義する. このとき, m のことを**反転量**と呼び, 「g **により 2 面体** i **は反転量** m **で辺** j **に移動した**」などという. $\diamond$

また, 系 3.1, 命題 3.1, 命題 3.2 に対応して以下が成り立つ. 証明も同様なので省略する.

系 3.2 $\forall g \in S_{48}, \forall i, j \in I_{12}, (g : E_i \rightsquigarrow E_j \ \Rightarrow\ g(E_i) = E_j)$[*6]. $\diamond$

命題 3.3 $\forall i \in I_{12}, \forall m_1, m_2 \in \mathbb{Z}_2, ((\forall k \in I_2, e(o_2{}^{m_1}(k), i) = e(o_2{}^{m_2}(k), i)) \ \Rightarrow\ m_1 = m_2)$. $\diamond$

命題 3.4 任意の $i, j, k \in I_{12},\ g, h \in S_{48}$ について, 以下の (1)〜(3) が成り立つ：

(1) $\varepsilon : E_i \rightsquigarrow E_i$.

(2) $g : E_i \rightsquigarrow E_j \ \Rightarrow\ g^{-1} : E_j \rightsquigarrow E_i$.

(3) $(g : E_i \rightsquigarrow E_j,\ h : E_j \rightsquigarrow E_k) \ \Rightarrow\ hg : E_i \rightsquigarrow E_k$. $\diamond$

4 ルービックキューブ群

4.1 ルービックキューブ群と規則を無視したルービックキューブ群

ルービックキューブに群論を導入するための第一歩となるのが, 以下の定理である.

定理 4.1 操作全体の集合

$$G \coloneqq \{x_1 x_2 \cdots x_n \mid n \in \mathbb{N}, x_i \in G_{\mathrm{b}}\}$$

と,

$$H \coloneqq \{\sigma \in S_{48} \mid (\forall i \in I_8, \exists j \in I_8, \sigma : C_i \rightsquigarrow C_j),\ (\forall i \in I_{12}, \exists j \in I_{12}, \sigma : E_i \rightsquigarrow E_j)\}$$

はともに S_{48} の部分群となる. $\diamond$

証明には, 以下の補題を用いる.

補題 4.1 任意の $\sigma \in S_{48}$ について, 以下の (1), (2) が成り立つ：

(1) $(\forall i \in I_8, \exists j \in I_8, \sigma : C_i \rightsquigarrow C_j) \ \Rightarrow\ (\exists! \pi \in S_8, \forall i \in I_8, \sigma : C_i \rightsquigarrow C_{\pi(i)})$.

(2) $(\forall i \in I_{12}, \exists j \in I_{12}, \sigma : E_i \rightsquigarrow E_j) \ \Rightarrow\ (\exists! \pi' \in S_{12}, \forall i \in I_{12}, \sigma : E_i \rightsquigarrow E_{\pi'(i)})$. $\diamond$

証明
任意に $\sigma \in S_{48}$ をとる.

(1) 任意に $i \in I_8$ をとると, 仮定よりある $j \in I_8$ が存在して $\sigma : C_i \rightsquigarrow C_j$ である. まず, 系 3.1 より $\sigma(C_i) = C_j$ であるから, i に対して j は一意に存在しなければならず, $\pi(i) = j$ なる $\pi : I_8 \to I_8$ がただ 1 つ存在する. さらに, σ は全単射なので π も全単射である.

(2) (1) と同様にして証明できる. ■

定理 4.1 の証明に入ろう.

[*6]ただし, 系 3.1 と違い逆も成り立つ. すなわち, 2 面体の場合は $g : E_i \rightsquigarrow E_j$ を $g(E_i) = E_j$ で代用可能だが, 反転量の考え方がいずれ必要になるのであえて導入している.

証明 [**定理 4.1**]

(G について) 定義より, G は積について閉じている. また, 任意の $x \in G_{\mathrm{b}}$ について $x^4 = \varepsilon$ なので, $x^{-1} = x^3$. したがって, 任意の G の元 $g = x_1 x_2 \cdots x_n$ $(x_i \in G_{\mathrm{b}})$ に対して, $g^{-1} = {x_n}^{-1} {x_{n-1}}^{-1} \cdots {x_1}^{-1} \in G$ とできる. これより単位元と逆元の存在がいえた.

(H について) まず, 任意に $h, h' \in H$ をとると, 任意の $i \in I_8$ に対してある $j \in I_8$ が存在して $h' : C_i \rightsquigarrow C_j$ である. さらに, j に対してもある $k \in I_8$ が存在して, $h : C_j \rightsquigarrow C_k$ となる. このとき, 命題 3.2 (3) より $hh' : C_i \rightsquigarrow C_k$ である. 同様にして, 任意の $i' \in I_{12}$ に対してある $k' \in I_{12}$ が存在して, $hh' : E_{i'} \rightsquigarrow E_{k'}$ も成立する. したがって H は積について閉じている.

また, 命題 3.2 (1), 3.4 (1) より任意の $i \in I_8$ および $i' \in I_{12}$ について $\varepsilon : C_i \rightsquigarrow C_i$, $\varepsilon : E_i \rightsquigarrow E_i$ が成り立つから, $\varepsilon \in H$ である.

最後に, 逆元の存在を示す. 任意に $h \in H$ をとると, 補題 4.1 よりある $\pi \in S_8$ が一意に存在して, $h : C_i \rightsquigarrow C_{\pi(i)}$ $(i \in I_8)$ である. 一方で, 命題 3.2 (2) より $h^{-1} \in S_{48}$ が $h^{-1} : C_{\pi(i)} \rightsquigarrow C_i$ $(i \in I_8)$ をみたす. ゆえに, $h^{-1} : C_i \rightsquigarrow C_{\pi^{-1}(i)}$ $(i \in I_8)$ となる. 同様にして, ある $\pi' \in S_{12}$ が一意に存在して, $h^{-1} : E_{i'} \rightsquigarrow E_{\pi'^{-1}(i')}$ $(i' \in I_{12})$ も成立する. したがって $h^{-1} \in H$ である. ■

ここで, 生成元の表記を用いれば $G = \langle R, L, U, D, F, B \rangle$ であり, G を**ルービックキューブ群**と呼ぶ. また H は, 小面の貼り替えを行わなず, 3 面体は 3 面体どうし, 2 面体は 2 面体どうしでしか置換しないという制約を S_{48} に課したものである. 言い換えると, H はルービックキューブの (1 面体を固定した) **分解と組み立て**の動作全体からなる集合とみなすことができる. そのような意味で, H を**規則を無視したルービックキューブ群**という. このとき, 以下の系が従う.

系 4.1 $G \subset H \subset S_{48}$. ◇

証明 全ての基本操作は H の元である：

- $R : C_2 \rightsquigarrow C_6, R : C_3 \rightsquigarrow C_2, R : C_6 \rightsquigarrow C_7, R : C_7 \rightsquigarrow C_3, R : C_i \rightsquigarrow C_i$ (その他の i),
  $R : E_2 \rightsquigarrow E_5, R : E_5 \rightsquigarrow E_{10}, R : E_6 \rightsquigarrow E_2, R : E_{10} \rightsquigarrow E_6, R : E_i \rightsquigarrow E_i$ (その他の i).
- $L : C_1 \rightsquigarrow C_4, L : C_4 \rightsquigarrow C_8, L : C_5 \rightsquigarrow C_1, L : C_8 \rightsquigarrow C_5, L : C_i \rightsquigarrow C_i$ (その他の i),
  $L : E_4 \rightsquigarrow E_7, L : E_7 \rightsquigarrow E_{12}, L : E_8 \rightsquigarrow E_4, L : E_{12} \rightsquigarrow E_8, L : E_i \rightsquigarrow E_i$ (その他の i).
- $U : C_1 \rightsquigarrow C_2, U : C_2 \rightsquigarrow C_3, U : C_3 \rightsquigarrow C_4, U : C_4 \rightsquigarrow C_1, U : C_i \rightsquigarrow C_i$ (その他の i),
  $U : E_1 \rightsquigarrow E_2, U : E_2 \rightsquigarrow E_3, U : E_3 \rightsquigarrow E_4, U : E_4 \rightsquigarrow E_1, U : E_i \rightsquigarrow E_i$ (その他の i).
- $D : C_5 \rightsquigarrow C_8, D : C_6 \rightsquigarrow C_5, D : C_7 \rightsquigarrow C_6, D : C_8 \rightsquigarrow C_7, D : C_i \rightsquigarrow C_i$ (その他の i),
  $D : E_9 \rightsquigarrow E_{12}, D : E_{10} \rightsquigarrow E_9, D : E_{11} \rightsquigarrow E_{10}, D : E_{12} \rightsquigarrow E_{11}, D : E_i \rightsquigarrow E_i$ (その他の i).
- $F : C_3 \rightsquigarrow C_7, F : C_4 \rightsquigarrow C_3, F : C_7 \rightsquigarrow C_8, F : C_8 \rightsquigarrow C_4, F : C_i \rightsquigarrow C_i$ (その他の i),
  $F : E_3 \rightsquigarrow E_6, F : E_6 \rightsquigarrow E_{11}, F : E_7 \rightsquigarrow E_3, F : E_{11} \rightsquigarrow E_7, F : E_i \rightsquigarrow E_i$ (その他の i).
- $B : C_1 \rightsquigarrow C_5, B : C_2 \rightsquigarrow C_1, B : C_5 \rightsquigarrow C_6, B : C_6 \rightsquigarrow C_2, B : C_i \rightsquigarrow C_i$ (その他の i),
  $B : E_1 \rightsquigarrow E_8, B : E_5 \rightsquigarrow E_1, B : E_8 \rightsquigarrow E_9, B : E_9 \rightsquigarrow E_5, B : E_i \rightsquigarrow E_i$ (その他の i).

したがって, G の任意の元もまた H の元である. ■

しかしながら, $G \neq H$ であることが 4.3 節で示される. すなわち, H の元の中に基本操作の積で表せないものが存在する[*7]. また, S_{48} そのものは分解と組み立てよりもさらに自由な, (1 面体以外の) 各小方体の小面の貼り替えの動作全体からなる集合とみなすことができる.

[*7]例えば, ある 1 つの 3 面体を時計まわりに 120 度 (無理やり) ひねると, そのルービックキューブはもはや規則に従った操作では一生揃わないものとなってしまう. すなわち, ある 1 つの 3 面体のみを時計まわりに 120 度回転し他のどの小方体も動かさない操作は存在しない.

4.2 H の群構造

この節では H の群としての構造を分析する. まずは, 以下の定理を示そう.

定理 4.2 集合 H と集合 $S_8 \times {\mathbb{Z}_3}^8 \times S_{12} \times {\mathbb{Z}_2}^{12}$ は 1 対 1 に対応する. $\diamond$

この定理は, Joyner[1](p.228) 定理 9.6.4(キューブ理論の第 1 基本定理) に相当するものであるが, 全ての 3 面体および 2 面体が配置される頂点および辺と, そのときの各小方体の面の向きを 1 つ定めることと, (1 面体を固定した) 分解と組み立ての動作を 1 つ定めることは同じことである, というのがこの定理の“心”である. 証明に入る前の下準備として, 以下の写像を定義する.

定義 4.1 任意に $h \in H$ をとると, 補題 4.1 より $\pi \in S_8$ が一意に存在して, $h : C_i \rightsquigarrow C_{\pi(i)}$ $(i \in I_8)$ である. このとき, 写像 φ を

$$\varphi : H \to S_8;\ h \mapsto \pi$$

で定める. さらに, 命題 3.1 より h と各 3 面体 i に対して回転量 n がただ 1 つ定まる. このとき, $t_i(h) \coloneqq n \in \mathbb{Z}_3$ とおいて, 写像 $\boldsymbol{t}$ を

$$\boldsymbol{t} : H \to {\mathbb{Z}_3}^8;\ h \mapsto (t_1(h), t_2(h), \ldots, t_8(h))$$

で定める. $\diamond$

定義 4.2 任意に $h \in H$ をとると, 補題 4.1 より $\pi' \in S_{12}$ が一意に存在して, $h : E_i \rightsquigarrow E_{\pi'(i)}$ $(i \in I_{12})$ である. このとき, 写像 ψ を

$$\psi : H \to S_{12};\ h \mapsto \pi'$$

で定める. さらに, 命題 3.3 より h と各 2 面体 i に対して反転量 m がただ 1 つ定まる. このとき, $f_i(h) \coloneqq m \in \mathbb{Z}_2$ とおいて, 写像 $\boldsymbol{f}$ を

$$\boldsymbol{f} : H \to {\mathbb{Z}_2}^{12};\ h \mapsto (f_1(h), f_2(h), \ldots, f_{12}(h))$$

で定める. $\diamond$

定義 4.3 写像 η を

$$\eta : H \to S_8 \times {\mathbb{Z}_3}^8 \times S_{12} \times {\mathbb{Z}_2}^{12};\ h \mapsto (\varphi(h), \boldsymbol{t}(h), \psi(h), \boldsymbol{f}(h))$$

で定める. $\diamond$

例 4.1 例えば, 各基本操作の像は以下のようになる：

- $\varphi(R) = (2\ 6\ 7\ 3),\ \boldsymbol{t}(R) = (0,2,1,0,0,1,2,0),$
  $\psi(R) = (2\ 5\ 10\ 6),\ \boldsymbol{f}(R) = (0,1,0,0,0,0,0,0,0,1,0,0).$
- $\varphi(L) = (1\ 4\ 8\ 5),\ \boldsymbol{t}(L) = (1,0,0,2,2,0,0,1),$
  $\psi(L) = (4\ 7\ 12\ 8),\ \boldsymbol{f}(L) = (0,0,0,0,0,0,1,1,0,0,0,0).$
- $\varphi(U) = (1\ 2\ 3\ 4),\ \boldsymbol{t}(U) = (0,0,0,0,0,0,0,0),$
  $\psi(U) = (1\ 2\ 3\ 4),\ \boldsymbol{f}(U) = (1,0,1,0,0,0,0,0,0,0,0,0).$
- $\varphi(D) = (5\ 8\ 7\ 6),\ \boldsymbol{t}(D) = (0,0,0,0,0,0,0,0),$
  $\psi(D) = (9\ 12\ 11\ 10),\ \boldsymbol{f}(D) = (0,0,0,0,0,0,0,0,0,1,0,1).$

- $\varphi(F) = (3\ 7\ 8\ 4),\ \boldsymbol{t}(F) = (0,0,2,1,0,0,1,2),$
  $\psi(F) = (3\ 6\ 11\ 7),\ \boldsymbol{f}(F) = (0,0,1,0,0,0,0,0,0,0,1,0).$
- $\varphi(B) = (1\ 5\ 6\ 2),\ \boldsymbol{t}(B) = (2,1,0,0,1,2,0,0),$
  $\psi(B) = (1\ 8\ 9\ 5),\ \boldsymbol{f}(B) = (0,0,0,0,1,0,0,1,0,0,0,0).$ $\diamond$

下準備は以上である. 定理 4.2 の証明に入ろう.

証明 [**定理 4.2**] 任意に $(\sigma, \boldsymbol{n}, \tau, \boldsymbol{m}) \in S_8 \times {\mathbb{Z}_3}^8 \times S_{12} \times {\mathbb{Z}_2}^{12}$ をとる. $\eta(h) = (\sigma, \boldsymbol{n}, \tau, \boldsymbol{m})$ なる $h \in H$ がただ 1 つ存在することを示そう.

$\boldsymbol{n} = (n_1, n_2, \ldots, n_8),\ \boldsymbol{m} = (m_1, m_2, \ldots, m_{12})$ とおく. いま,

$$C_{\mathrm{all}} = C_{\sigma(1)} \cup C_{\sigma(2)} \cup \cdots \cup C_{\sigma(8)},\ E_{\mathrm{all}} = E_{\tau(1)} \cup E_{\tau(2)} \cup \cdots \cup E_{\tau(12)}$$

であって, さらに任意に $i \in I_8$ および $i' \in I_{12}$ をとると,

$$C_{\sigma(i)} = \{c({o_3}^{n_i}(k), \sigma(i)) \mid k \in I_3\},\ E_{\tau(i')} = \{e({o_2}^{m_{i'}}(k), \tau(i')) \mid k \in I_2\}$$

となるから,

$$h(c(k,i)) = c({o_3}^{n_i}(k), \sigma(i))\ (k \in I_3),\ h(e(k,i')) = e({o_2}^{m_{i'}}(k), \tau(i'))\ (k \in I_2)$$

をみたす $h \in S_{48}$ がただ 1 つとれる. このとき, $h : C_i \rightsquigarrow C_{\sigma(i)}$ かつ $h : E_{i'} \rightsquigarrow E_{\tau(i')}$ より $h \in H$ である. 一方, 定義より $\sigma = \varphi(h),\ n_i = t_i(h),\ \tau = \psi(h),\ m_{i'} = f_{i'}(h)$ なので, $(\sigma, \boldsymbol{n}, \tau, \boldsymbol{m}) = \eta(h)$ となる. ■

さて, 群の構造の対応まで知るためには, さらに積 $hh' \in H$ の η による像を調べる必要がある. まず, 以下の写像を定義しよう.

定義 4.4 写像 $\iota : S_n \to \mathrm{Map}({\mathbb{Z}_m}^n, {\mathbb{Z}_m}^n);\ \sigma \mapsto \iota_\sigma$ を, $\boldsymbol{k} = (k_1, k_2, \ldots, k_n) \in {\mathbb{Z}_m}^n$ に対して

$$\iota_\sigma(\boldsymbol{k}) \coloneqq (k_{\sigma(1)}, k_{\sigma(2)}, \ldots, k_{\sigma(n)})$$

で定める. ここで, ι は厳密には n, m に依存するが, 簡単のために全ての n, m に対して ι と表記することとする. $\diamond$

以降, ${\mathbb{Z}_m}^n$ は直積群であるとする. このとき, $\eta(hh')$ について以下のことが分かる.

命題 4.1 任意の $h, h' \in H$ に対して, 以下の (1)〜(4) が成り立つ:

(1) $\varphi(hh') = \varphi(h)\varphi(h').$

(2) $\boldsymbol{t}(hh') = \iota_{\varphi(h')}(\boldsymbol{t}(h)) + \boldsymbol{t}(h').$

(3) $\psi(hh') = \psi(h)\psi(h').$

(4) $\boldsymbol{f}(hh') = \iota_{\psi(h')}(\boldsymbol{f}(h)) + \boldsymbol{f}(h').$ $\diamond$

証明

任意に $h, h' \in H$ をとる.

(1) $\sigma \coloneqq \varphi(h),\ \sigma' \coloneqq \varphi(h')$ とおく. まず, 任意の $i \in I_8$ について $h' : C_i \rightsquigarrow C_{\sigma'(i)},\ h : C_{\sigma'(i)} \rightsquigarrow C_{\sigma\sigma'(i)}$. よって命題 3.2 (3) より, $hh' : C_i \rightsquigarrow C_{\sigma\sigma'(i)}$. 一方で, 定義より $\varphi(hh') = \sigma\sigma' = \varphi(h)\varphi(h')$.

(2) 任意に $i \in I_8$ をとり, $j \coloneqq \varphi(h')(i)$, $k \coloneqq \varphi(h)(j)$ とおく. $t_i(hh') = t_j(h) + t_i(h')$ を示せばよい. 任意の $l \in I_3$ について,

$$\begin{aligned} hh'(c(l,i)) &= h(c({o_3}^{t_i(h')}(l), j)) \\ &= c({o_3}^{t_j(h)}({o_3}^{t_i(h')}(l)), k) \\ &= c({o_3}^{t_j(h)+t_i(h')}(l), \varphi(hh')(i)) \ (\because (1)). \end{aligned}$$

一方で, 定義より $t_i(hh') = t_j(h) + t_i(h')$ となる (図 4.1).

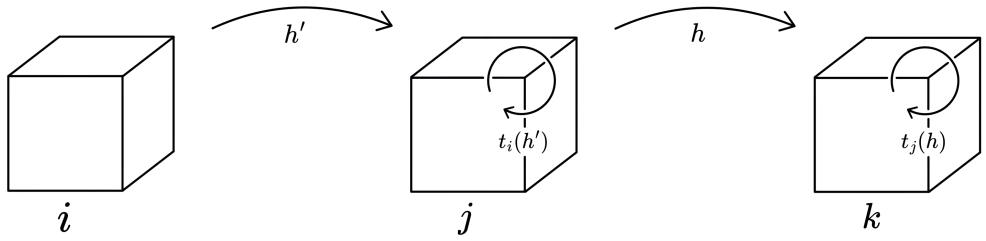

図 4.1 3 面体の回転量の推移

(3), (4) 同様にして証明できる. ■

命題 4.1 より, 残念ながら η は群 H から直積群 $S_8 \times {\mathbb{Z}_3}^8 \times S_{12} \times {\mathbb{Z}_2}^{12}$ への同型ではない. ところで, ι は以下の性質を持つ.

命題 4.2 以下の (1)〜(3) が成り立つ：

(1) $\forall \boldsymbol{k} \in {\mathbb{Z}_m}^n, \iota_\varepsilon(\boldsymbol{k}) = \boldsymbol{k}$.

(2) $\forall \sigma \in S_n, \forall \boldsymbol{k}, \boldsymbol{k}' \in {\mathbb{Z}_m}^n, \iota_\sigma(\boldsymbol{k} + \boldsymbol{k}') = \iota_\sigma(\boldsymbol{k}) + \iota_\sigma(\boldsymbol{k}')$.

(3) $\forall \sigma, \sigma' \in S_n, \iota_{\sigma\sigma'} = \iota_{\sigma'}\iota_\sigma$. ◇

証明

(1) 任意の $\boldsymbol{k} = (k_1, k_2, \ldots, k_n) \in {\mathbb{Z}_m}^n$ について $\iota_\varepsilon(\boldsymbol{k}) = (k_{\varepsilon(1)}, k_{\varepsilon(2)}, \ldots, k_{\varepsilon(n)}) = \boldsymbol{k}$.

(2) 任意に $\sigma \in S_n$ および $\boldsymbol{k} = (k_1, k_2, \ldots, k_n)$, $\boldsymbol{k}' = ({k'}_1, {k'}_2, \ldots, {k'}_n) \in {\mathbb{Z}_m}^n$ をとると,

$$\begin{aligned} \iota_\sigma(\boldsymbol{k} + \boldsymbol{k}') &= (k_{\sigma(1)} + {k'}_{\sigma(1)}, k_{\sigma(2)} + {k'}_{\sigma(2)}, \ldots, k_{\sigma(n)} + {k'}_{\sigma(n)}) \\ &= \iota_\sigma(\boldsymbol{k}) + \iota_\sigma(\boldsymbol{k}'). \end{aligned}$$

(3) 任意に $\sigma, \sigma' \in S_n$ をとると, 任意の $\boldsymbol{k} = (k_1, k_2, \ldots, k_n) \in {\mathbb{Z}_m}^n$ について

$$\begin{aligned} \iota_{\sigma\sigma'}(\boldsymbol{k}) &= (k_{\sigma(\sigma'(1))}, k_{\sigma(\sigma'(2))}, \ldots, k_{\sigma(\sigma'(n))}) \\ &= \iota_{\sigma'}(k_{\sigma(1)}, k_{\sigma(2)}, \ldots, k_{\sigma(n)}) \\ &= \iota_{\sigma'}\iota_\sigma(\boldsymbol{k}). \end{aligned}$$

よって, $\iota_{\sigma\sigma'} = \iota_{\sigma'}\iota_\sigma$ である. ■

命題 4.2 から, ι は準同型 $\iota : S_n \to (\mathrm{Aut}({\mathbb{Z}_m}^n))^{\mathrm{op}}$ であることが分かる. そしてこのことから, η の像と対応する演算もまた集合 $S_8 \times {\mathbb{Z}_3}^8 \times S_{12} \times {\mathbb{Z}_2}^{12}$ 上に群構造を与えることが導かれる.

定理 4.3 集合 $S_n \times {\mathbb{Z}_m}^n$ 上の積を

$$(\sigma, \boldsymbol{k})(\sigma', \boldsymbol{k}') \coloneqq (\sigma\sigma', \iota_{\sigma'}(\boldsymbol{k}) + \boldsymbol{k}') \ ((\sigma, \boldsymbol{k}), (\sigma', \boldsymbol{k}') \in S_n \times {\mathbb{Z}_m}^n)$$

で定めると, この演算により集合 $S_n \times {\mathbb{Z}_m}^n$ は群となる. ◇

証明 任意に $(\sigma, \boldsymbol{k}) \in S_n \times {\mathbb{Z}_m}^n$ をとると,

$$(\varepsilon, \mathbf{0}_n)(\sigma, \boldsymbol{k}) = (\varepsilon\sigma, \iota_\sigma(\mathbf{0}_n) + \boldsymbol{k}) = (\sigma, \mathbf{0}_n + \boldsymbol{k}) = (\sigma, \boldsymbol{k}),$$
$$(\sigma, \boldsymbol{k})(\varepsilon, \mathbf{0}_n) = (\sigma\varepsilon, \iota_\varepsilon(\boldsymbol{k}_n) + \mathbf{0}_n) = (\sigma, \boldsymbol{k} + \mathbf{0}_n) = (\sigma, \boldsymbol{k})$$

より, $(\varepsilon, \mathbf{0}_n) \in S_n \times {\mathbb{Z}_m}^n$ は単位元であり,

$$(\sigma^{-1}, \iota_{\sigma^{-1}}(-\boldsymbol{k}))(\sigma, \boldsymbol{k}) = (\sigma^{-1}\sigma, \iota_\sigma(\iota_{\sigma^{-1}}(-\boldsymbol{k})) + \boldsymbol{k}) = (\varepsilon, (-\boldsymbol{k}) + \boldsymbol{k}) = (\varepsilon, \mathbf{0}_n),$$
$$(\sigma, \boldsymbol{k})(\sigma^{-1}, \iota_{\sigma^{-1}}(-\boldsymbol{k})) = (\sigma\sigma^{-1}, \iota_{\sigma^{-1}}(\boldsymbol{k}) + \iota_{\sigma^{-1}}(-\boldsymbol{k})) = (\varepsilon, \iota_{\sigma^{-1}}(\boldsymbol{k} + (-\boldsymbol{k}))) = (\varepsilon, \mathbf{0}_n)$$

より, $(\sigma^{-1}, \iota_{\sigma^{-1}}(-\boldsymbol{k})) \in S_n \times {\mathbb{Z}_m}^n$ は $(\sigma, \boldsymbol{k})$ の逆元である.

また, 任意に $(\sigma_1, \boldsymbol{k}_1), (\sigma_2, \boldsymbol{k}_2), (\sigma_3, \boldsymbol{k}_3) \in S_n \times {\mathbb{Z}_m}^n$ をとると,

$$\begin{aligned}((\sigma_1, \boldsymbol{k}_1)(\sigma_2, \boldsymbol{k}_2))(\sigma_3, \boldsymbol{k}_3) &= (\sigma_1\sigma_2, \iota_{\sigma_2}(\boldsymbol{k}_1) + \boldsymbol{k}_2)(\sigma_3, \boldsymbol{k}_3)\\ &= ((\sigma_1\sigma_2)\sigma_3, \iota_{\sigma_3}(\iota_{\sigma_2}(\boldsymbol{k}_1) + \boldsymbol{k}_2) + \boldsymbol{k}_3)\\ &= (\sigma_1(\sigma_2\sigma_3), \iota_{\sigma_2\sigma_3}(\boldsymbol{k}_1) + (\iota_{\sigma_3}(\boldsymbol{k}_2) + \boldsymbol{k}_3))\\ &= (\sigma_1, \boldsymbol{k}_1)(\sigma_2\sigma_3, \iota_{\sigma_3}(\boldsymbol{k}_2) + \boldsymbol{k}_3)\\ &= (\sigma_1, \boldsymbol{k}_1)((\sigma_2, \boldsymbol{k}_2)(\sigma_3, \boldsymbol{k}_3))\end{aligned}$$

より, 結合則も成り立つ. ■

ι により定められた上記の群を, 直積群 $S_n \times {\mathbb{Z}_m}^n$ と区別するために $S_n \ltimes_\iota {\mathbb{Z}_m}^n$ とかき, (外部) **半直積**と呼ぶ[*8]. 以降, 簡単のため単に $S_n \ltimes {\mathbb{Z}_m}^n$ とかくこととする. そして, 定理 4.2, 命題 4.1, 定理 4.3 からの帰結として以下の定理を得る.

定理 4.4 $H \cong S_8 \ltimes {\mathbb{Z}_3}^8 \times S_{12} \ltimes {\mathbb{Z}_2}^{12}$[*9]. ◇

証明 $\eta : H \to S_8 \ltimes {\mathbb{Z}_3}^8 \times S_{12} \ltimes {\mathbb{Z}_2}^{12}$ は, 定理 4.2 より全単射で, かつ命題 4.1, 定理 4.3 から任意の $h, h' \in H$ に対して

$$\begin{aligned}\eta(hh') &= (\varphi(h)\varphi(h'),\ \iota_{\varphi(h')}(\boldsymbol{t}(h)) + \boldsymbol{t}(h'),\ \psi(h)\psi(h'),\ \iota_{\psi(h')}(\boldsymbol{f}(h)) + \boldsymbol{f}(h'))\\ &= (\varphi(h), \boldsymbol{t}(h), \psi(h), \boldsymbol{f}(h))\ (\varphi(h'), \boldsymbol{t}(h'), \psi(h'), \boldsymbol{f}(h'))\\ &= \eta(h)\eta(h')\end{aligned}$$

より準同型である. ■

4.3 G の群構造

前節の結果をもとに, G の群構造も分析しよう. まず, 以下の集合を定義する.

定義 4.5 $G' \subset S_8 \ltimes {\mathbb{Z}_3}^8 \times S_{12} \ltimes {\mathbb{Z}_2}^{12}$ を以下で定義する.

$$G' := \{(\sigma, \boldsymbol{n}, \tau, \boldsymbol{m}) \in S_8 \ltimes {\mathbb{Z}_3}^8 \times S_{12} \ltimes {\mathbb{Z}_2}^{12} \mid (4.1), (4.2), (4.3)\}$$

ここで, $\boldsymbol{n} = (n_1, n_2, \ldots, n_8),\ \boldsymbol{m} = (m_1, m_2, \ldots, m_{12})$ に対し

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau), \tag{4.1}$$
$$n_1 + n_2 + \cdots + n_8 = 0, \tag{4.2}$$
$$m_1 + m_2 + \cdots + m_{12} = 0. \quad \diamond \tag{4.3}$$

[*8] 一般には, 群 H, N と準同型 $\phi : H \to (\mathrm{Aut}(N))^{\mathrm{op}}$ に対して同様に (外部) 半直積 $H \ltimes_\phi N$ が定義される.

[*9] $S_8 \ltimes {\mathbb{Z}_3}^8 \times S_{12} \ltimes {\mathbb{Z}_2}^{12}$ は集合として $S_8 \times {\mathbb{Z}_3}^8 \times S_{12} \times {\mathbb{Z}_2}^{12}$ と同じで, その演算を $S_8 \times {\mathbb{Z}_3}^8$ と $S_{12} \times {\mathbb{Z}_2}^{12}$ のそれぞれに対応する成分について半直積の演算として定めたもの.

この集合に関して, 以下の命題が成り立つ.

命題 4.3 G' は ${S_8} \ltimes {\mathbb{Z}_3}^8 \times {S_{12}} \ltimes {\mathbb{Z}_2}^{12}$ の部分群である. $\diamond$

証明 まず, G' が積で閉じていることを示す. 任意に $(\sigma, \boldsymbol{n}, \tau, \boldsymbol{m}), (\sigma', \boldsymbol{n}', \tau', \boldsymbol{m}') \in G'$ をとると, sgn は準同型だから

$$\mathrm{sgn}(\sigma\sigma') = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma') = \mathrm{sgn}(\tau)\mathrm{sgn}(\tau') = \mathrm{sgn}(\tau\tau').$$

また, $\boldsymbol{n}, \boldsymbol{n}'$ の i 成分 $n_i, {n'}_i$ について,

$$\sum_{i \in I_8} (n_{\sigma'(i)} + {n'}_i) = \sum_{i \in I_8} n_{\sigma'(i)} + \sum_{i \in I_8} {n'}_i = \sum_{i \in I_8} n_i + \sum_{i \in I_8} {n'}_i = 0.$$

同様に, $\boldsymbol{m}, \boldsymbol{m}'$ の i 成分 $m_i, {m'}_i$ について,

$$\sum_{i \in I_{12}} (m_{\tau'(i)} + {m'}_i) = \sum_{i \in I_{12}} m_{\tau'(i)} + \sum_{i \in I_{12}} {m'}_i = \sum_{i \in I_{12}} m_i + \sum_{i \in I_{12}} {m'}_i = 0.$$

したがって, 積 $(\sigma, \boldsymbol{n}, \tau, \boldsymbol{m})(\sigma', \boldsymbol{n}', \tau', \boldsymbol{m}') = (\sigma\sigma', \iota_{\sigma'}(\boldsymbol{n}) + \boldsymbol{n}', \tau\tau', \iota_{\tau'}(\boldsymbol{m}) + \boldsymbol{m}')$ は (4.1)〜(4.3) を満たすので, G' は積で閉じている.

また, $\mathrm{sgn}(\varepsilon) = \mathrm{sgn}(\varepsilon) = 1$ であり, $\boldsymbol{0}_8, \boldsymbol{0}_{12}$ も (4.2), (4.3) を満たすので, ${S_8} \ltimes {\mathbb{Z}_3}^8 \times {S_{12}} \ltimes {\mathbb{Z}_2}^{12}$ の単位元 $(\varepsilon, \boldsymbol{0}_8, \varepsilon, \boldsymbol{0}_{12})$ は G' の元である.

さらに, 任意の $(\sigma, \boldsymbol{n}, \tau, \boldsymbol{m}) \in {S_8} \ltimes {\mathbb{Z}_3}^8 \times {S_{12}} \ltimes {\mathbb{Z}_2}^{12}$ の逆元 $(\sigma^{-1}, \iota_{\sigma^{-1}}(-\boldsymbol{n}), \tau^{-1}, \iota_{\tau^{-1}}(-\boldsymbol{m}))$ も,

$$\begin{aligned}
&\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau) = \mathrm{sgn}(\tau^{-1}),\\
&\sum_{i \in I_8} (-n_{\sigma^{-1}(i)}) = -\sum_{i \in I_8} n_{\sigma^{-1}(i)} = -\sum_{i \in I_8} n_i = 0,\\
&\sum_{i \in I_{12}} (-m_{\tau^{-1}(i)}) = -\sum_{i \in I_{12}} m_{\tau^{-1}(i)} = -\sum_{i \in I_{12}} m_i = 0
\end{aligned}$$

より (4.1)〜(4.3) を満たすので, G' の元であることが分かる. ■

唐突に登場した G' だが, 実はこれが G の群構造を与える.

定理 4.5 $G \cong G'$. $\diamond$

この定理は, Joyner[1](p.276) 定理 11.2.2(キューブ理論の第 2 基本定理) に相当するものである. 証明に入る前に, 以下の補題を用意する.

補題 4.2 以下の (1), (2) が成り立つ:

(1) 任意の長さ 3 の巡回置換 $\rho \in S_8, \rho' \in S_{12}$ に対して,

$$\eta(g) = (\rho, \boldsymbol{t}(g), \varepsilon, \boldsymbol{f}(g)),\ \eta(g') = (\varepsilon, \boldsymbol{t}(g'), \rho', \boldsymbol{f}(g'))$$

なる $g, g' \in G$ が存在する.

(2) 任意の $i \in I_7$ および $i' \in I_{11}$ に対して,

$$\eta(g) = (\varepsilon, \boldsymbol{x}_i, \varepsilon, \boldsymbol{0}_{12}),\ \eta(g') = (\varepsilon, \boldsymbol{0}_8, \varepsilon, {\boldsymbol{x}'}_{i'})$$

なる $g, g' \in G$ が存在する. ただし,

$$\boldsymbol{x}_i \coloneqq (\ldots, \underbrace{1}_{i\text{ 成分}}, \ldots, 2) \in {\mathbb{Z}_3}^8,\ {\boldsymbol{x}'}_{i'} \coloneqq (\ldots, \underbrace{1}_{i'\text{成分}}, \ldots, 1) \in {\mathbb{Z}_2}^{12}$$

($\ldots$ の成分は全て 0). $\diamond$

この補題の証明には以下の操作を用いる.

定義 4.6 操作 $C_\mathrm{p}, E_\mathrm{p}, C_\mathrm{o}, E_\mathrm{o} \in G$ を,

$$
\begin{aligned}
C_\mathrm{p} &\coloneqq [UL^{-1}U^{-1}, R],\\
E_\mathrm{p} &\coloneqq [L^{-1}U^2L, R^{-1}F^2R],\\
C_\mathrm{o} &\coloneqq [[U,R]^2, L^2],\\
E_\mathrm{o} &\coloneqq [LBR^2L^2F^2R^{-1}LU, L^2]
\end{aligned}
$$

で定める. それぞれ, **CP 操作**, **EP 操作**, **CO 操作**, **EO 操作**と呼ぶ. ◇

まず, これらの操作で何ができるのかを確認しよう.

命題 4.4 定義 4.6 の 4 つの操作について, 以下が成り立つ：

$$
\begin{aligned}
\eta(C_\mathrm{p}) &= ((1\ 2\ 3), \boldsymbol{t}(C_\mathrm{p}), \varepsilon, \boldsymbol{f}(C_\mathrm{p})),\\
\eta(E_\mathrm{p}) &= (\varepsilon, \boldsymbol{t}(E_\mathrm{p}), (1\ 3\ 11), \boldsymbol{f}(E_\mathrm{p})),\\
\eta(C_\mathrm{o}) &= (\varepsilon, (1,0,0,0,0,0,0,2), \varepsilon, \mathbf{0}_{12}),\\
\eta(E_\mathrm{o}) &= (\varepsilon, \mathbf{0}_8, \varepsilon, (0,0,0,1,0,0,0,0,0,0,0,1)).
\end{aligned}
\quad ◇
$$

証明 ルービックキューブを回すことで確認できる. ■

これらの操作の“成り立ち”に関しては次節で説明する. ひとまず, これらの操作を用いて補題 4.2 を示そう.

証明 [**補題 4.2**]

(1) 任意に長さ 3 の巡回置換 $\rho = (i_1\ i_2\ i_3) \in S_8,\ \rho' = (i'_1\ i'_2\ i'_3) \in S_{12}$ をとる. いま, $g_\rho, g_{\rho'} \in G$ をそれぞれ

$$
\varphi(g_\rho) = \begin{pmatrix} i_1 & i_2 & i_3 \\ 1 & 2 & 3 \end{pmatrix} \sigma_\rho,\ \psi(g_{\rho'}) = \begin{pmatrix} i'_1 & i'_2 & i'_3 \\ 1 & 3 & 11 \end{pmatrix} \sigma_{\rho'}
$$

を満たすようにとる (ただし, σ_ρ は $\{i_1, i_2, i_3\}$ 以外の置換, $\sigma_{\rho'}$ は $\{i'_1, i'_2, i'_3\}$ 以外の置換を表す). このような操作がいつでも存在することは, ルービックキューブを回すことで容易に確認できる. このとき,

$$
\begin{aligned}
&\varphi({g_\rho}^{-1} C_\mathrm{p} g_\rho) = {\sigma_\rho}^{-1} \begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix} (1\ 2\ 3) \begin{pmatrix} i_1 & i_2 & i_3 \\ 1 & 2 & 3 \end{pmatrix} \sigma_\rho = {\sigma_\rho}^{-1} (i_1\ i_2\ i_3) \sigma_\rho = \rho,\\
&\psi({g_\rho}^{-1} C_\mathrm{p} g_\rho) = \psi(g_\rho)^{-1} \varepsilon \psi(g_\rho) = \varepsilon
\end{aligned}
$$

かつ

$$
\begin{aligned}
&\varphi({g_{\rho'}}^{-1} E_\mathrm{p} g_{\rho'}) = \varphi(g_{\rho'})^{-1} \varepsilon \varphi(g_{\rho'}) = \varepsilon,\\
&\psi({g_{\rho'}}^{-1} E_\mathrm{p} g_{\rho'}) = {\sigma_{\rho'}}^{-1} \begin{pmatrix} 1 & 3 & 11 \\ i'_1 & i'_2 & i'_3 \end{pmatrix} (1\ 3\ 11) \begin{pmatrix} i'_1 & i'_2 & i'_3 \\ 1 & 3 & 11 \end{pmatrix} \sigma_{\rho'} = {\sigma_{\rho'}}^{-1} (i'_1\ i'_2\ i'_3) \sigma_{\rho'} = \rho'
\end{aligned}
$$

であるから, $g = {g_\rho}^{-1} C_\mathrm{p} g_\rho,\ g' = {g_{\rho'}}^{-1} E_\mathrm{p} g_{\rho'}$ とすればよい (図 4.2, 図 4.3).

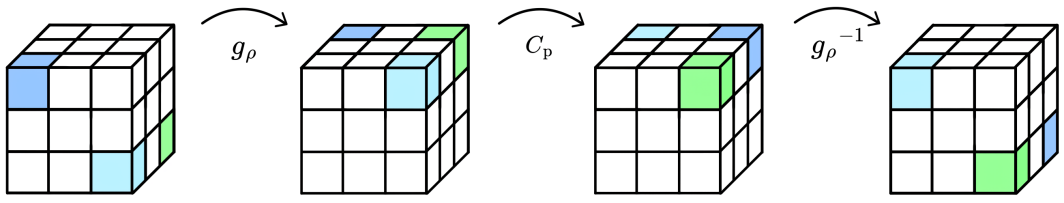

図 4.2 $\rho = (4\ 6\ 7)$ の場合の 3 面体の移動

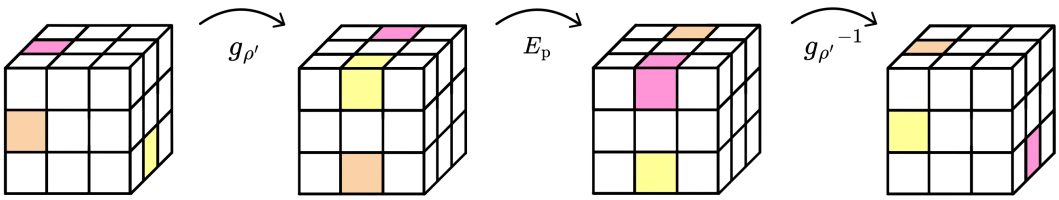

図 4.3 $\rho' = (4\ 10\ 7)$ の場合の 2 面体の移動

(2) 任意に $i \in I_7$ および $i' \in I_{11}$ をとる. いま, $g_i, g_{i'} \in G$ をそれぞれ

$$\varphi(g_i) = \begin{pmatrix} i & 8 \\ 1 & 8 \end{pmatrix} \sigma_i,\ \psi(g_{i'}) = \begin{pmatrix} i' & 12 \\ 4 & 12 \end{pmatrix} \sigma_{i'}$$

を満たすようにとる (ただし, σ_i は $\{i, 8\}$ 以外の置換, $\sigma_{i'}$ は $\{i', 12\}$ 以外の置換を表す). このような操作がいつでも存在することは, ルービックキューブを回すことで容易に確認できる. このとき, まず

$$\begin{aligned}
&\varphi({g_i}^{-1} C_{\mathrm{o}} g_i) = \varphi(g_i)^{-1} \varepsilon \varphi(g_i) = \varepsilon,\ \psi({g_i}^{-1} C_{\mathrm{o}} g_i) = \psi(g_i)^{-1} \varepsilon \psi(g_i) = \varepsilon, \\
&\varphi({g_{i'}}^{-1} E_{\mathrm{o}} g_{i'}) = \varphi(g_{i'})^{-1} \varepsilon \varphi(g_{i'}) = \varepsilon,\ \psi({g_{i'}}^{-1} E_{\mathrm{o}} g_{i'}) = \psi(g_{i'})^{-1} \varepsilon \psi(g_{i'}) = \varepsilon
\end{aligned}$$

である. また,

$$\begin{aligned}
t_i({g_i}^{-1} C_{\mathrm{o}} g_i) &= t_1({g_i}^{-1} C_{\mathrm{o}}) + t_i(g_i) = t_1({g_i}^{-1}) + t_1(C_{\mathrm{o}}) + t_i(g_i) = 1 + t_i({g_i}^{-1} g_i) = 1, \\
t_8({g_i}^{-1} C_{\mathrm{o}} g_i) &= t_8({g_i}^{-1} C_{\mathrm{o}}) + t_8(g_i) = t_8({g_i}^{-1}) + t_8(C_{\mathrm{o}}) + t_8(g_i) = 2 + t_8({g_i}^{-1} g_i) = 2
\end{aligned}$$

かつ, 任意の $j \in I_8 \setminus \{i, 8\}$ に対して

$$t_j({g_i}^{-1} C_{\mathrm{o}} g_i) = t_{\sigma_i(j)}({g_i}^{-1} C_{\mathrm{o}}) + t_j(g_i) = t_{\sigma_i(j)}({g_i}^{-1}) + t_{\sigma_i(j)}(C_{\mathrm{o}}) + t_j(g_i) = t_j({g_i}^{-1} g_i) = 0$$

が成り立つので, $\boldsymbol{t}({g_i}^{-1} C_{\mathrm{o}} g_i) = \boldsymbol{x}_i$ であり,

$$\begin{aligned}
\boldsymbol{f}({g_i}^{-1} C_{\mathrm{o}} g_i) &= \iota_{\psi(g_i)}(\boldsymbol{f}({g_i}^{-1} C_{\mathrm{o}})) + \boldsymbol{f}(g_i) = \iota_{\psi(g_i)}(\boldsymbol{f}({g_i}^{-1}) + \boldsymbol{f}(C_{\mathrm{o}})) + \boldsymbol{f}(g_i) \\
&= \iota_{\psi(g_i)}(\boldsymbol{f}({g_i}^{-1})) + \boldsymbol{f}(g_i) = \boldsymbol{f}({g_i}^{-1} g_i) = \boldsymbol{0}_{12}
\end{aligned}$$

も成り立つ. さらに,

$$\begin{aligned}
\boldsymbol{t}({g_{i'}}^{-1} E_{\mathrm{o}} g_{i'}) &= \iota_{\varphi(g_{i'})}(\boldsymbol{t}({g_{i'}}^{-1} E_{\mathrm{o}})) + \boldsymbol{t}(g_{i'}) = \iota_{\varphi(g_{i'})}(\boldsymbol{t}({g_{i'}}^{-1}) + \boldsymbol{t}(E_{\mathrm{o}})) + \boldsymbol{t}(g_{i'}) \\
&= \iota_{\varphi(g_{i'})}(\boldsymbol{t}({g_{i'}}^{-1})) + \boldsymbol{t}(g_{i'}) = \boldsymbol{t}({g_{i'}}^{-1} g_{i'}) = \boldsymbol{0}_8
\end{aligned}$$

であり,

$$\begin{aligned}
f_{i'}({g_{i'}}^{-1} E_{\mathrm{o}} g_{i'}) &= f_4({g_{i'}}^{-1} E_{\mathrm{o}}) + f_{i'}(g_{i'}) = f_4({g_{i'}}^{-1}) + f_4(E_{\mathrm{o}}) + f_{i'}(g_{i'}) \\
&= 1 + f_{i'}({g_{i'}}^{-1} g_{i'}) = 1, \\
f_{12}({g_{i'}}^{-1} E_{\mathrm{o}} g_{i'}) &= f_{12}({g_{i'}}^{-1} E_{\mathrm{o}}) + f_{12}(g_{i'}) = f_{12}({g_{i'}}^{-1}) + f_{12}(E_{\mathrm{o}}) + f_{12}(g_{i'}) \\
&= 1 + f_{12}({g_{i'}}^{-1} g_{i'}) = 1
\end{aligned}$$

かつ, 任意の $j' \in I_{12} \setminus \{i', 12\}$ に対して

$$\begin{aligned}
f_{j'}({g_{i'}}^{-1} E_{\mathrm{o}} g_{i'}) &= f_{\sigma_{i'}(j')}({g_{i'}}^{-1} E_{\mathrm{o}}) + f_{j'}(g_{i'}) = f_{\sigma_{i'}(j')}({g_{i'}}^{-1}) + f_{\sigma_{i'}(j')}(E_{\mathrm{o}}) + f_{j'}(g_{i'}) \\
&= f_{j'}({g_{i'}}^{-1} g_{i'}) = 0
\end{aligned}$$

が成り立つので, $\boldsymbol{f}({g_{i'}}^{-1} E_{\mathrm{o}} g_{i'}) = {\boldsymbol{x}'}_{i'}$ である. 以上より, $g = {g_i}^{-1} C_{\mathrm{o}} g_i,\ g' = {g_{i'}}^{-1} E_{\mathrm{o}} g_{i'}$ とすればよい (図 4.4, 図 4.5). ■

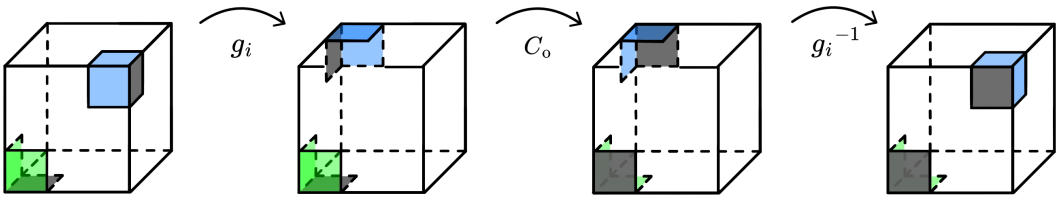

図 4.4 $i = 3$ の場合の 3 面体の回転

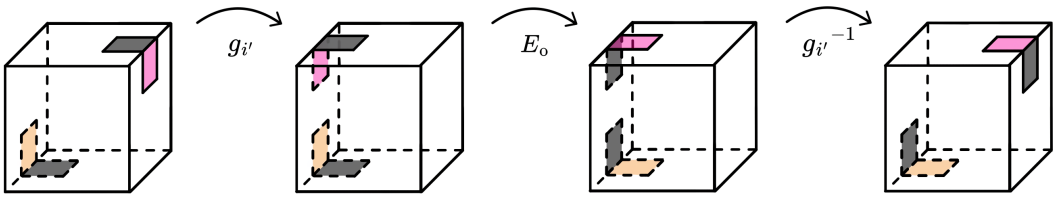

図 4.5 $i' = 2$ の場合の 2 面体の反転

最後に, 補題の証明中に登場した操作にも名前をつける.

定義 4.7 補題 4.2 (1) の証明で登場した 2 つの操作を

$$C_\mathrm{p}(\rho) \coloneqq {g_\rho}^{-1} C_\mathrm{p} g_\rho,\ E_\mathrm{p}(\rho') \coloneqq {g_{\rho'}}^{-1} E_\mathrm{p} g_{\rho'}$$

とかき, これらをそれぞれ**一般化 CP 操作**, **一般化 EP 操作**と呼ぶ.

また, 補題 4.2 (2) の証明で登場した 2 つの操作を

$$C_\mathrm{o}(i) \coloneqq {g_i}^{-1} C_\mathrm{o} g_i,\ E_\mathrm{o}(i') \coloneqq {g_{i'}}^{-1} E_\mathrm{o} g_{i'}$$

とかき, これらをそれぞれ**一般化 CO 操作**, **一般化 EO 操作**と呼ぶ. ◇

以上の定義および補題を用いて, 定理 4.5 の証明をしよう.

証明 [定理 4.5] $\eta|_G : G \to S_8 \ltimes {\mathbb{Z}_3}^8 \times S_{12} \ltimes {\mathbb{Z}_2}^{12}$ が, G から G' への同型となっていることを示す. η は同型なので, $\eta|_G(G) = G'$ を示せばよい.

($\eta|_G(G) \subset G'$ について) 任意に $y \in \eta|_G(G)$ をとると, ある $x_i \in G_\mathrm{b}$ $(i \in I_n)$ があって $y = \eta|_G(x_1 x_2 \cdots x_n)$. ここで, 例 4.1 より $\eta|_G(x_i) \in G'$ $(i \in I_n)$ であるから, $\eta|_G$ が準同型であることと, G' が積で閉じていることに注意して,

$$\eta|_G(x_1 x_2 \cdots x_n) = \eta|_G(x_1)\eta|_G(x_2)\cdots\eta|_G(x_n) \in G'.$$

ゆえに, $\eta|_G(G) \subset G'$ である.

($\eta|_G(G) \supset G'$ について) 任意に $g' = (\sigma, \boldsymbol{n}, \tau, \boldsymbol{m}) \in G'$ をとる ($\boldsymbol{n} = (n_1, n_2, \ldots, n_8)$, $\boldsymbol{m} = (m_1, m_2, \ldots, m_{12})$ とする).

(1) $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau) = -1$ **のとき**

$\varphi(R) = (2\ 6\ 7\ 3)$ と $\psi(R) = (2\ 5\ 10\ 6)$ が奇置換であることから,

$$\sigma = (2\ 6\ 7\ 3)\sigma_1\sigma_2\cdots\sigma_N,\ \tau = (2\ 5\ 10\ 6)\tau_1\tau_2\cdots\tau_M$$

なる長さ 3 の巡回置換 $\sigma_1, \sigma_2, \ldots, \sigma_N \in S_8$, $\tau_1, \tau_2, \ldots, \tau_M \in S_{12}$ がとれる. まず, $p \in G$ を

$$p \coloneqq RC_\mathrm{p}(\sigma_1)C_\mathrm{p}(\sigma_2)\cdots C_\mathrm{p}(\sigma_N)E_\mathrm{p}(\tau_1)E_\mathrm{p}(\tau_2)\cdots E_\mathrm{p}(\tau_M)$$

で定めると, 補題 4.2 (1) より

$$\begin{aligned}\varphi(p) &= \varphi(R)\varphi(C_{\mathrm{p}}(\sigma_1))\varphi(C_{\mathrm{p}}(\sigma_2))\cdots\varphi(C_{\mathrm{p}}(\sigma_N))\varphi(E_{\mathrm{p}}(\tau_1))\varphi(E_{\mathrm{p}}(\tau_2))\cdots\varphi(E_{\mathrm{p}}(\tau_M))\\ &= (2\ 6\ 7\ 3)\sigma_1\sigma_2\cdots\sigma_N = \sigma,\\ \psi(p) &= \psi(R)\psi(C_{\mathrm{p}}(\sigma_1))\psi(C_{\mathrm{p}}(\sigma_2))\cdots\psi(C_{\mathrm{p}}(\sigma_N))\psi(E_{\mathrm{p}}(\tau_1))\psi(E_{\mathrm{p}}(\tau_2))\cdots\psi(E_{\mathrm{p}}(\tau_M))\\ &= (2\ 5\ 10\ 6)\tau_1\tau_2\cdots\tau_M = \tau\end{aligned}$$

であるから,

$$\eta|_G(p) = (\sigma, \boldsymbol{t}(p), \tau, \boldsymbol{f}(p)) \tag{4.4}$$

となる.

次に, $o \in G$ を

$$\begin{aligned}o \coloneqq\ & C_{\mathrm{o}}(1)^{-t_1(p)+n_1}C_{\mathrm{o}}(2)^{-t_2(p)+n_2}\cdots C_{\mathrm{o}}(7)^{-t_7(p)+n_7}\\ & E_{\mathrm{o}}(1)^{-f_1(p)+m_1}E_{\mathrm{o}}(2)^{-f_2(p)+m_2}\cdots E_{\mathrm{o}}(11)^{-f_{11}(p)+m_{11}}\end{aligned}$$

で定めると, 補題 4.2 (2) より

$$\begin{aligned}&\varphi(o) = \varepsilon,\ \psi(o) = \varepsilon,\\ &t_i(o) = -t_i(p) + n_i\ (i \in I_7),\ f_i(o) = -f_i(p) + m_i\ (i \in I_{11}).\end{aligned}$$

したがって, (4.4) より,

$$\begin{aligned}&\varphi(po) = \varphi(p)\varphi(o) = \sigma,\ \psi(po) = \psi(p)\psi(o) = \tau,\\ &t_i(po) = t_{\varepsilon(i)}(p) + t_i(o) = t_i(p) + (-t_i(p) + n_i) = n_i\ (i \in I_7),\\ &f_i(po) = f_{\varepsilon(i)}(p) + f_i(o) = f_i(p) + (-f_i(p) + m_i) = m_i\ (i \in I_{11})\end{aligned}$$

となる. ここで $po \in G$ なので, $\eta|_G(G) \subset G'$ から $\eta|_G(po) \in G'$. よって (4.2), (4.3) に注意すると

$$\begin{aligned}t_8(po) &= -\sum_{i\in I_7} t_i(po) = -\sum_{i\in I_7} n_i = n_8,\\ f_{12}(po) &= -\sum_{i\in I_{11}} f_i(po) = -\sum_{i\in I_{11}} m_i = m_{12}.\end{aligned}$$

ゆえに, $(\sigma, \boldsymbol{n}, \tau, \boldsymbol{m}) = \eta|_G(po) \in \eta|_G(G)$ となる.

(2) $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau) = 1$ **のとき**

このときは,

$$\sigma = \sigma_1\sigma_2\cdots\sigma_N,\ \tau = \tau_1\tau_2\cdots\tau_M$$

なる長さ 3 の巡回置換 $\sigma_1, \sigma_2, \ldots, \sigma_N \in S_8,\ \tau_1, \tau_2, \ldots, \tau_M \in S_{12}$ がとれる. ゆえに,

$$\begin{aligned}p' &\coloneqq C_{\mathrm{p}}(\sigma_1)C_{\mathrm{p}}(\sigma_2)\cdots C_{\mathrm{p}}(\sigma_N)E_{\mathrm{p}}(\tau_1)E_{\mathrm{p}}(\tau_2)\cdots E_{\mathrm{p}}(\tau_M),\\ o' &\coloneqq C_{\mathrm{o}}(1)^{-t_1(p')+n_1}C_{\mathrm{o}}(2)^{-t_2(p')+n_2}\cdots C_{\mathrm{o}}(7)^{-t_7(p')+n_7}\\ &\qquad E_{\mathrm{o}}(1)^{-f_1(p')+m_1}E_{\mathrm{o}}(2)^{-f_2(p')+m_2}\cdots E_{\mathrm{o}}(11)^{-f_{11}(p')+m_{11}}\end{aligned}$$

とすれば, (1) と同様にして, $(\sigma, \boldsymbol{n}, \tau, \boldsymbol{m}) = \eta|_G(p'o') \in \eta|_G(G)$ となる. ■

上記の証明で登場した po や $p'o'$ は, 完成状態のルービックキューブを定義 4.5 の条件を満たす任意の模様に変える操作であるから, 任意の模様のルービックキューブは理論上これらの逆写像によって完成させることができる[*10]. そして定理 4.5 の系として, G の位数, すなわちルービックキューブの模様の総数を求めることができる.

系 4.2 $|G| = 8! \times 3^7 \times 12! \times 2^{10} = 43,252,003,274,489,856,000.$ $\diamond$

証明 定理 4.5 より $|G| = |G'|$ であるから, G' の元の個数を ${S_8} \ltimes {\mathbb{Z}_3}^8 \times {S_{12}} \ltimes {\mathbb{Z}_2}^{12}$ に制約を付ける形で数え上げる.

まず置換の総数について, $S_8 \times S_{12}$ は, (S_8 の元, S_{12} の元) の置換の偶奇の組合せ (偶, 偶),(偶, 奇),(奇, 偶),(奇, 奇) によって互いに置換の総数が等しいの 4 通りに分けられる. このうち (4.1) を満たすのは 2 通りなので, 置換の総数は $\frac{2}{4}|S_8 \times S_{12}| = \frac{1}{2} \times 8! \times 12!$ 通りである.

また 3 面体の回転量の総数は, ${\mathbb{Z}_3}^8$ において 7 つの $\mathbb{Z}_3$ の元を定めた時点で, 8 つ目の元は (4.2) より決まるので自由に選べるのは ${\mathbb{Z}_3}^7$ の分だけであり, 3^7 通りである. 2 面体の反転量の総数についても同様に考えて, (4.3) より 2^{11} 通りである.

以上より, $|G'| = \frac{1}{2} \times 8! \times 12! \times 3^7 \times 2^{11} = 8! \times 3^7 \times 12! \times 2^{10}$ となる. ■

5 交換子

5.1 交換子による作用

この節では, 交換子の作用に関する一般論を述べる. 以下, $\sigma, \tau \in S_n$ に対し

$$S(\sigma,\tau) \coloneqq \mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau),\ C(\sigma,\tau) \coloneqq S(\sigma,\tau) \cup \sigma^{-1}S(\sigma,\tau) \cup \tau^{-1}S(\sigma,\tau)$$

とおく. まずは以下の補題から示そう.

補題 5.1 $\forall \sigma,\tau \in S_n, \forall i \in I_n, ((i \in \mathrm{supp}(\sigma) \wedge i \notin \sigma^{-1}S(\sigma,\tau)) \Rightarrow \tau(\sigma(i)) = \sigma(i)).$ $\diamond$

証明 任意に $\sigma, \tau \in S_n$ および $i \in I_n$ をとる. まず, $\sigma(i) \notin S(\sigma,\tau)$ より, $\sigma(i) \notin \mathrm{supp}(\sigma)$ または $\sigma(i) \notin \mathrm{supp}(\tau)$, すなわち $\sigma(\sigma(i)) = \sigma(i)$ または $\tau(\sigma(i)) = \sigma(i)$ である. ところが, $i \in \mathrm{supp}(\sigma)$ から $\sigma(i) \neq i$, すなわち $\sigma(\sigma(i)) \neq \sigma(i)$ であるから, $\tau(\sigma(i)) = \sigma(i)$. ■

交換子と $C(\sigma,\tau)$ に関して, 以下の命題が成り立つ.

命題 5.1 $\forall \sigma,\tau \in S_n, \forall i \in I_n \setminus C(\sigma,\tau), [\sigma,\tau](i) = i.$ $\diamond$

証明 任意に $\sigma, \tau \in S_n$ および $i \in I_n \setminus C(\sigma,\tau)$ をとる. $i \notin S(\sigma,\tau)$ に注意して, 以下の 3 つの場合に分けて考える.

($i \notin \mathrm{supp}(\sigma)$ **かつ** $i \notin \mathrm{supp}(\tau)$ **のとき**) $\sigma(i) = \tau(i) = i$ より, $[\sigma,\tau](i) = \tau^{-1}\sigma^{-1}\tau\sigma(i) = i.$

($i \in \mathrm{supp}(\sigma)$ **かつ** $i \notin \mathrm{supp}(\tau)$ **のとき**) $i \notin \sigma^{-1}S(\sigma,\tau)$ から, 補題 5.1 より $\tau(\sigma(i)) = \sigma(i)$, すなわち $\sigma^{-1}\tau\sigma(i) = i$ である. さらに, $\tau(i) = i$ なので, $[\sigma,\tau](i) = \tau^{-1}(\sigma^{-1}\tau\sigma(i)) = \tau^{-1}i = i.$

($i \notin \mathrm{supp}(\sigma)$ **かつ** $i \in \mathrm{supp}(\tau)$ **のとき**) 上記と同様にして証明できる. ■

この命題から, 交換子 $[\sigma,\tau]$ によって変化し得るのは $C(\sigma,\tau)$ の元のみということになる. さらに, $C(\sigma,\tau)$ に然るべき仮定を課すことによって, 交換子による元の挙動をある程度制御することができる.

[*10] 定義 4.7 の各操作の逆写像もまた, 定義 4.7 の各操作であるから, R^{-1}(奇置換の操作ならなんでもよい) と一般化 CP 操作, 一般化 EP 操作, 一般化 CO 操作, 一般化 EO 操作によってルービックキューブは完成させられるということになる.

定理 5.1 任意に $\sigma, \tau \in S_n$ をとる．$S(\sigma,\tau) = \{k\}$ のとき，$[\sigma,\tau] \in S_n$ は以下の (1)〜(3) を満たす：

(1) $[\sigma,\tau](k) = \tau^{-1}(k)$.

(2) $[\sigma,\tau](\tau^{-1}(k)) = \sigma^{-1}(k)$.

(3) $[\sigma,\tau](\sigma^{-1}(k)) = k$. $\diamond$

証明 任意に $\sigma, \tau \in S_n$ をとり，$S(\sigma,\tau) = \{k\}$ とする．

(1) $k \in \mathrm{supp}(\sigma)$ より $\sigma(k) \neq k$ だから，$\sigma(k) \notin S(\sigma,\tau)$．ゆえに，補題 5.1 より $\tau(\sigma(k)) = \sigma(k)$，すなわち $\sigma^{-1}\tau\sigma(k) = k$ であるから，$[\sigma,\tau](k) = \tau^{-1}(\sigma^{-1}\tau\sigma(k)) = \tau^{-1}(k)$.

(2) $k \in \mathrm{supp}(\tau) = \mathrm{supp}(\tau^{-1})$ より $\tau^{-1}(k) \neq k$ だから，$\tau^{-1}(k) \notin S(\sigma,\tau) = S(\tau^{-1},\sigma)$．ゆえに，補題 5.1 より $\sigma(\tau^{-1}(k)) = \tau^{-1}(k)$，すなわち $\tau\sigma\tau^{-1}(k) = k$ である．同様に，$k \in \mathrm{supp}(\sigma^{-1})$ と $\sigma^{-1}(k) \notin S(\sigma^{-1},\tau^{-1})$ から，補題 5.1 より $\tau^{-1}(\sigma^{-1}(k)) = \sigma^{-1}(k)$ である．
以上より，$[\sigma,\tau](\tau^{-1}(k)) = \tau^{-1}\sigma^{-1}(\tau\sigma\tau^{-1}(k)) = \tau^{-1}\sigma^{-1}(k) = \sigma^{-1}(k)$.

(3) $[\tau,\sigma]$ に (1) を適用することで，$[\tau,\sigma](k) = \sigma^{-1}(k)$．ゆえに，$[\sigma,\tau](\sigma^{-1}(k)) = k$. ■

命題 5.1 と合わせて，定理 5.1 の仮定のもとで $[\sigma,\tau]$ は巡回置換 $(k\ \tau^{-1}(k)\ \sigma^{-1}(k))$ と等しいことが分かる．さらに $[\sigma,\tau]$ は偶置換であるから，例えば $\tau^{-1}(k) \neq k$ に注意すれば $[\sigma,\tau]$ は長さ 3 の巡回置換となることが分かる．
また，別の仮定を $C(\sigma,\tau)$ に課して考えてみる．

定理 5.2 任意に $\sigma, \tau \in S_n$ をとる．$S(\sigma,\tau) = \sigma^{-1}S(\sigma,\tau) \neq \varnothing$ かつ $S(\sigma,\tau) \cap \tau^{-1}S(\sigma,\tau) = \varnothing$ のとき，$[\sigma,\tau] \in S_n$ は以下の (1), (2) を満たす：

(1) $\forall i \in S(\sigma,\tau), [\sigma,\tau](i) \in S(\sigma,\tau)$.

(2) $\forall i \in \tau^{-1}S(\sigma,\tau), [\sigma,\tau](i) \in \tau^{-1}S(\sigma,\tau)$. $\diamond$

証明 任意に $\sigma, \tau \in S_n$ をとり，$S(\sigma,\tau) = \sigma^{-1}S(\sigma,\tau) \neq \varnothing$ かつ $S(\sigma,\tau) \cap \tau^{-1}S(\sigma,\tau) = \varnothing$ とする．

(1) 任意に $i \in S(\sigma,\tau) = \sigma^{-1}S(\sigma,\tau)$ をとると，$\sigma(i) \in S(\sigma,\tau)$ より $\sigma(i) \in \mathrm{supp}(\tau)$ であって，$S(\sigma,\tau) \cap \tau^{-1}S(\sigma,\tau) = \varnothing$ から $\sigma(i) \notin \tau^{-1}S(\tau,\sigma^{-1})$ なので，補題 5.1 より $\sigma^{-1}(\tau(\sigma(i))) = \tau(\sigma(i))$，すなわち $\tau^{-1}\sigma^{-1}\tau\sigma(i) = \sigma(i)$ である．よって，$[\sigma,\tau](i) = \sigma(i) \in S(\sigma,\tau)$.

(2) 任意に $i \in \tau^{-1}S(\sigma,\tau)$ をとる．このとき，$\tau(i) \in S(\sigma,\tau)$ より $\sigma^{-1}\tau(i) \in \sigma^{-1}S(\sigma,\tau) = S(\sigma,\tau)$ となる．また，$i \notin S(\sigma,\tau)$ であることと，$\tau(\tau(i)) \neq \tau(i)$ より $\tau(i) \neq i$ となることから，$\sigma(i) = i$ である．よって，$[\sigma,\tau](i) = \tau^{-1}\sigma^{-1}\tau\sigma(i) = \tau^{-1}(\sigma^{-1}\tau(i)) \in \tau^{-1}S(\sigma,\tau)$. ■

命題 5.1 と合わせて，定理 5.2 の仮定のもとで $[\sigma,\tau]$ は $S(\sigma,\tau)$ から $S(\sigma,\tau)$ への全単射の部分と，$\tau^{-1}S(\sigma,\tau)$ から $\tau^{-1}S(\sigma,\tau)$ への全単射の部分に分割されることが分かる．

5.2 交換子による操作の構成

前節の内容に基づいて，交換子を用いて定義 4.6 の操作を構成してみよう．準備として，$\Phi(g) : I_{20} \to I_{20}$ を

$$\Phi(g)(i) = \begin{cases} \varphi(g)(i) & (1 \leq i \leq 8) \\ \psi(g)(i-8)+8 & (9 \leq i \leq 20) \end{cases}$$

で定める. このとき, $\Phi(g) \in S_{20}$ であり, g によって 3 面体 i は頂点 $\Phi(g)(i) = \varphi(g)(i)$ に移動し, 2 面体 i は $\Phi(g)(i+8) - 8 = \psi(g)(i)$ に移動することが分かる. 言い換えれば $\Phi(g)$ は, $g \in G$ による 3 面体および 2 面体の位置の (向きは無視した) 置換を表す S_{20} の元である. また, φ, ψ の準同型性から $\Phi : G \to S_{20};\ g \mapsto \Phi(g)$ の準同型が従う. そして, $\Phi(g), \Phi(h) \in S_{20}$ が定理 5.1 の仮定を満たすように $g, h \in G$ をとれば, $[g, h]$ によってある 3 つの 3 面体あるいは 2 面体のみの巡回置換を表現することができる.

例 5.1 C_{p} と E_{p} の構成手順は, 以下の通りである：

(C_{p} の構成) $\sigma \coloneqq \Phi(UL^{-1}U^{-1}),\ \tau \coloneqq \Phi(R)$ とおくと,

$$S(\sigma, \tau) = \{2\},\ \sigma^{-1}(2) = 1,\ \tau^{-1}(2) = 3.$$

よって定理 5.1 より, $[\sigma, \tau] = \Phi([UL^{-1}U^{-1}, R]) = \Phi(C_{\mathrm{p}}) = (1\ 2\ 3)$ であるから,

$$\eta(C_{\mathrm{p}}) = ((1\ 2\ 3), \boldsymbol{t}(C_{\mathrm{p}}), \varepsilon, \boldsymbol{f}(C_{\mathrm{p}}))$$

が従う.

(E_{p} の構成) $\sigma \coloneqq \Phi(L^{-1}U^2L),\ \tau \coloneqq \Phi(R^{-1}F^2R)$ とおくと,

$$S(\sigma, \tau) = \{11\},\ \sigma^{-1}(11) = 9,\ \tau^{-1}(11) = 19.$$

よって定理 5.1 より, $[\sigma, \tau] = \Phi([L^{-1}U^2L, R^{-1}F^2R]) = \Phi(E_{\mathrm{p}}) = (9\ 11\ 19)$ であるから,

$$\eta(E_{\mathrm{p}}) = (\varepsilon, \boldsymbol{t}(E_{\mathrm{p}}), (1\ 3\ 11), \boldsymbol{f}(E_{\mathrm{p}}))$$

が従う. $\diamond$

また, C_{o} と E_{o} については位置と向きの両方を考慮する必要があるため, $g, h \in G$ を定理 5.2 の仮定を満たすようにとることとなる.

例 5.2 C_{o} と E_{o} の構成手順は, 以下の通りである：

(C_{o} の構成) $g \coloneqq [U, R]^2,\ h \coloneqq L^2$ とおくと,

$$S(g, h) = g^{-1}S(g, h) = C_1,\ h^{-1}S(g, h) = C_8.$$

よって定理 5.2 より, $[g, h](C_1) = C_1$ かつ $[g, h](C_8) = C_8$. さらに, $f_1([g, h]) = 1,\ f_8([g, h]) = 2$ であるから,

$$\eta(C_{\mathrm{o}}) = (\varepsilon, (1, 0, 0, 0, 0, 0, 0, 2), \varepsilon, \mathbf{0}_{12}).$$

が従う.

(E_{o} の構成) $g \coloneqq LBR^2L^2F^2R^{-1}LU,\ h \coloneqq L^2$ とおくと,

$$S(g, h) = g^{-1}S(g, h) = E_4,\ h^{-1}S(g, h) = E_{12}.$$

よって定理 5.2 より, $[g, h](E_4) = E_4$ かつ $[g, h](E_{12}) = E_{12}$. さらに, $t_4([g, h]) = 1,\ t_{12}([g, h]) = 1$ であるから,

$$\eta(E_{\mathrm{o}}) = (\varepsilon, \mathbf{0}_8, \varepsilon, (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)).$$

が従う. $\diamond$

6　結び

本レポートでは, 操作と置換の同一視から始まり, [1] を叩き台にしつつ独自の概念も導入して, 最終的にはルービックキューブ群の位数という形でルービックキューブの模様のパターンの総数を求めることができた. その過程で, 半直積の概念も理解することができた. ルービックキューブ群の位数を求めるために, 本質的にルービックキューブを解く操作を数式上で構成する必要があったことには非常に驚いたが, 早解きを趣味とする私からすればとても楽しい議論であった.

謝辞

本レポートの作成にあたり, 専門外の研究分野でありながら指導教員として熱心な指導をして下さった桂田 祐史准教授には深く感謝申し上げます.

参考文献

[1] Joyner, D., 『群論の味わい — 置換群で解き明かすルービックキューブと 15 パズル —』, 川辺 治之（訳）, 共立出版 (2010).

[2] 株式会社トライボックス, “3 × 3 × 3 回転記号”, TORIBO (2024-03-05), https://tribox.com/3x3x3/solution/notation/ (参照 2024-08-01).

[3] 齋藤 正彦, 『線型代数入門』, 東京大学出版会 (1966).

[4] 雪江 明彦, 『代数学 1 群論入門 [第 2 版]』, 日本評論社 (2023).

[5] 佐藤 隆夫, 『シローの定理』, 近代科学社 (2015).

[6] 真中 遥道, “半直積を知ろう（無料記事）”, note (2024-06-20), https://note.com/manaka_kamogawa/n/n0b98728824e2 (参照 2024-11-22).

[7] 松本 眞, “代数系への入門 モノイド・群・環” (2020-09-24), http://www.math.sci.hiroshima-u.ac.jp/m-mat/TEACH/daisu-nyumon20191010-2.pdf (参照 2024-11-25).

[8] Koskivirta, J. S., “代数学 C・代数学特論 III 2023 年度前期” (2024-04-01), https://www.rimath.saitama-u.ac.jp/lab.jp/koskivirta/teaching/Saitama/2023_zenki_daisuu_C_kougi.pdf (参照 2024-12-06).

[9] うすい, “え!! 交換子だけでルービックキューブを!?”, Mathlog (2023-08-06), https://mathlog.info/articles/tvqptXmidRSDkBFDqLN5 (参照 2025-01-23).

A　群の基本

本稿において前提となる群論に関する内容をまとめた. 今までに登場した記号を別の意味で使用している箇所があるが, あくまで本文とは隔離した場所ということでご了承願いたい.

A.1　群の定義と例

集合 A 上の (2 項) **演算**とは, 写像 $\varphi : A \times A \to A$ のことをいう. 写像を演算とみなすとき, 通常は演算を表す適当な記号 $*$ を用いて, $\varphi(a,b) = a * b$ などとかく. 演算 $\varphi : A \times A \to A$ が定められたとき, A は演算 φ について**閉じている**という[*11].

定義 A.1 空でない集合 G 上で定義された演算 $*$ が,

(1) $\exists e \in G, \forall g \in G, e * g = g * e = g$. (**単位元の存在**)

(2) $\forall g \in G, \exists g' \in G, g' * g = g * g' = e$.[*12] (**逆元の存在**)

(3) $\forall g_1, g_2, g_3 \in G, (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$. (**結合則**)

を満たすとき, 組 $(G, *)$ を**群**と呼ぶ. さらに

(4) $\forall g_1, g_2 \in G, g_1 * g_2 = g_2 * g_1$. (**交換則**)

を満たすときは, 組 $(G, *)$ を**可換群** (あるいはアーベル群) と呼ぶ. 着目している演算が明らかなときには, 単に G のことを群や可換群と呼ぶ. ◇

(1) の e を G の単位元, (2) の g' を g の逆元と呼ぶ. **加法**と呼ばれる演算 (演算記号は $+$, $g+g'$ を g と g' の**和**と呼ぶ) を考えているときは, 単位元を 0_G, 逆元を $-g$ などとかく. 一方で**乗法**と呼ばれる演算 (演算記号は $\cdot$[*13], $g \cdot g'$ を g と g' の**積**と呼ぶ) を考えているときは, 単位元を 1_G, 逆元を g^{-1} などとかく. 以降特に断りのない限り, 一般的な群は全て乗法による群として記述する.

例 A.1 $I_n \coloneqq \{1, 2, \ldots, n\}$ とする. $S_n \coloneqq \{\sigma : I_n \to I_n \mid \sigma \text{ は全単射 }\}$ は, 写像の合成 (以降写像の積とも呼ぶ) によって群となる. ◇

証明 2 つの全単射を合成しても全単射なので, S_n は合成について閉じている. また, 単位元は恒等写像, 逆元は逆写像に対応し, 結合則は明らかである. ■

例 A.2 $\mathbb{Z}_n \coloneqq \{0, 1, \ldots, n-1\}$ は, n を法とする加法によって群となる. これを n **を法とする剰余群**と呼ぶ. ◇

証明 通常の加法と区別するため, ここでのみ $x, y \in \mathbb{Z}_n$ に対し $x + y$ を n で割った余りが r であることを, $x \dot{+} y = r$ とかく. すると, $\mathbb{Z}_n$ は明らかに $\dot{+}$ について閉じていて, 単位元は 0, 任意の $x \in \mathbb{Z}_n$ の逆元は $n - x \in \mathbb{Z}_n$ である. また, $(x \dot{+} y) \dot{+} z$, $x \dot{+} (y \dot{+} z)$ $(x, y, z \in \mathbb{Z}_n)$ はいずれも, $x + y + z$ を n で割った余りであるから, 結合則も成り立つ. ■

[*11] 言い換えれば, 演算の結果がまた A の中に収まっているときのこと.
[*12] e は (1) に登場する e と同じ.
[*13] しばしば省略される.

A.2　対称群の性質

定義 A.2 例 A.1 の S_n を n **次対称群**と呼ぶ. S_n の元のことを (n 次の) **置換**と呼び, $\sigma \in S_n$ を

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

とかく. 特に, I_n から I_n への恒等写像を**恒等置換**と呼ぶ.

また, ある 2 以上の $m \in I_n$ と相異なる $i_1, i_2, \ldots, i_m \in I_n$ があって,

$$\sigma(i_k) = i_{k+1}\ (k \in I_{m-1}),\ \sigma(i_m) = i_1,$$
$$\sigma(j) = j\ (j \in I_n \setminus I_{m-1})$$

となるとき, σ を**長さ** m **の巡回置換**といい,

$$\sigma = (i_1\ i_2\ \cdots\ i_m)$$

とかく. 長さ 2 の巡回置換は**互換**と呼ばれる. $\diamond$

注意 A.1 指定されていない数字に関しては全て恒等的に置換するものとして, 次数の異なる置換を同一視することができる. 例えば,

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in S_2,\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$$

は異なる置換であるが, 元の対応を見れば同じ置換と考えても問題ない. 実際, これらを等しく (1 2) と表記するわけである. $\diamond$

命題 A.1 任意の置換は有限個の互換の積で表現できる. $\diamond$

証明 S_n $(n = 1, 2, \ldots)$ ごとに, n に関する帰納法で示す.

$n = 1$ のとき, まず S_1 の元を S_n $(n \geq 2)$ における恒等置換と同一視すると, これは互換の積として表現できる (例えば $(1\ 2)^2$).

ある n で仮定して $n+1$ のとき, 任意に $\sigma \in S_{n+1}$ をとる. $\sigma(n+1) = n+1$ のときは, $\sigma \in S_n$ とみなせるので, 仮定より σ は有限個の互換の積で表現できる. 一方 $\sigma(n+1) \neq n+1$ のときは, $\sigma(n+1) = m$ とおくと $(n+1\ m)\sigma(n+1) = n+1$ であるから, $(n+1\ m)\sigma \in S_n$ とみなせる. $(n+1\ m)\sigma = \tau$ とおくと, $\sigma = (n+1\ m)\tau$ となるから, 仮定より σ は有限個の互換の積で表現できる. ■

互換の積への分解の仕方は 1 通りではないが, 以下の定理が成り立つ.

定理 A.1 置換を有限個の互換の積で表現したとき, 積に現れる互換の個数の偶奇は置換に対して一意に定まる. $\diamond$

証明 多項式

$$f(x_1, x_2, \ldots, x_n) \coloneqq \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

を考え, $\sigma \in S_n$ に対して,

$$f^\sigma(x_1, x_2, \ldots, x_n) \coloneqq f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

と定める. このとき, $\tau \in S_n$ が互換であるとすると f の定義より

$$f^\tau(x_1, x_2, \ldots, x_n) \coloneqq -f(x_1, x_2, \ldots, x_n)$$

である. いま, 任意にとった $\sigma \in S_n$ が 2 通りの互換の積として $\sigma = \tau_1\tau_2 \dots \tau_N = \rho_1\rho_2 \dots \rho_M$ と表現されているとすると,

$$f^\sigma(x_1, x_2, \dots, x_n) = (-1)^N f(x_1, x_2, \dots, x_n) = (-1)^M f(x_1, x_2, \dots, x_n)$$

ゆえ, $(-1)^N = (-1)^M$. よって N, M の偶奇は一致する. ■

置換が偶数個の互換の積で表現されるとき**偶置換**, 奇数個の互換の積で表現されるとき**奇関数**と呼ぶ. さらに, 次の写像が定義できる.

定義 A.3 符号関数 sgn を

$$\mathrm{sgn} : S_n \to \{-1, 1\};\ \sigma \mapsto \mathrm{sgn}(\sigma) \coloneqq \begin{cases} 1 & (\sigma \text{ は偶置換}) \\ -1 & (\sigma \text{ は奇置換}) \end{cases}$$

で定める. ◇

また, 以下の系はルービックキューブ論に必要となる.

系 A.1 任意の奇置換 $\sigma, \tau \in S_n$ に対して,

$$\sigma = \tau\rho_1\rho_2 \cdots \rho_N$$

なる長さ 3 の巡回置換 $\rho_1, \rho_2, \dots, \rho_N \in S_n$ が存在する. ◇

証明 まず, 任意の 2 つの互換の積は有限個の長さ 3 の巡回置換の積になる：

$$(i\ j)(i\ j) = (i\ j\ k)^3,\ (i\ j)(i\ k) = (i\ k\ j),\ (i\ j)(k\ l) = (i\ k\ j)(i\ k\ l).$$

ゆえに, 偶置換は有限個の長さ 3 の巡回置換の積で表現されることがわかる.

いま, 任意に奇置換 $\sigma, \tau \in S_n$ をとると, τ^{-1} は奇置換なので, $\tau^{-1}\sigma$ は偶置換である. ゆえに,

$$\tau^{-1}\sigma = \rho_1\rho_2 \cdots \rho_N$$

なる長さ 3 の巡回置換 $\rho_1, \rho_2, \dots, \rho_N \in S_n$ をとることができて, 両辺に左から τ をかければ目的の式を得る. ■

B 群の性質

B.1 正規部分群

定義 B.1 群 G の部分集合 H が G と同じ演算によって群になるとき, H を G の**部分群**という. ◇

命題 B.1 群 G の部分集合 H が G の部分群であるための必要十分条件は, 以下の (1)〜(3) が成立することである：

(1) $\forall g, h \in G, gh \in H$.

(2) $1_G \in H$.

(3) $\forall h \in H, h^{-1} \in H$. ◇

結合則の確認は, 自明ゆえに不必要となる. 部分群の中でも, 以下の正規部分群と呼ばれるものは様々な役割を果たす.

定義 B.2 群 G の部分群 N が, $gng^{-1} \in N$ $(g \in G,\ n \in N)$ を満たすとき, N を G の**正規部分群**といい, $N \triangleleft G$ あるいは $G \triangleright N$ とかく. ◇

B.2　群の準同型と同型

定義 B.3 A, B は群であるとする．写像 $\varphi : A \to B$ が，

$$\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)\ (a_1, a_2 \in A)$$

を満たしているとき，φ を**準同型写像**あるいは**準同型**と呼ぶ．特に φ が準同型かつ全単射であるときには，φ を**同型写像**あるいは**同型**と呼び，$A \cong B$ とかく．このとき，A と B は同型であるという．　◇

例 B.1 $\mathrm{sgn} : S_n \to \{-1, 1\}$ は準同型である．ただし，$\{-1, 1\}$ は通常の実数の積についての群とみなす．　◇

証明 $\sigma_{\mathrm{ev}} \in S_n$ を偶置換，$\sigma_{\mathrm{od}} \in S_n$ を奇置換とすると，$\sigma_{\mathrm{ev}}\sigma_{\mathrm{ev}}$，$\sigma_{\mathrm{od}}\sigma_{\mathrm{od}}$ は偶置換，$\sigma_{\mathrm{ev}}\sigma_{\mathrm{od}}$，$\sigma_{\mathrm{od}}\sigma_{\mathrm{ev}}$ は奇置換であるから，

$$\mathrm{sgn}(\sigma_{\mathrm{ev}}\sigma_{\mathrm{ev}}) = \mathrm{sgn}(\sigma_{\mathrm{od}}\sigma_{\mathrm{od}}) = 1,\ \mathrm{sgn}(\sigma_{\mathrm{ev}}\sigma_{\mathrm{od}}) = \mathrm{sgn}(\sigma_{\mathrm{od}}\sigma_{\mathrm{ev}}) = -1.$$

一方，$\mathrm{sgn}(\sigma_{\mathrm{ev}}) = 1,\ \mathrm{sgn}(\sigma_{\mathrm{od}}) = -1$ なので，sgn は準同型となる．　■

命題 B.2 A, B を群とし，$\varphi : A \to B$ は準同型であるとする．このとき，以下の (1), (2) が成り立つ：

(1) $\varphi(1_A) = 1_B$.

(2) $\forall a \in A, \varphi(a^{-1}) = \varphi(a)^{-1}$.　◇

証明

(1) $\varphi(1_A) = \varphi(1_A 1_A) = \varphi(1_A)\varphi(1_A)$ より，$\varphi(1_A) = 1_B$.

(2) 任意に $a \in A$ をとると，(1) より $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1_A) = 1_B$．ゆえに $\varphi(a^{-1}) = \varphi(a)^{-1}$．　■

定義 B.4 群 G から群 G への同型を G の**自己同型**といい，G の自己同型全体からなる集合を $\mathrm{Aut}(G)$ とかく．写像の合成によって $\mathrm{Aut}(G)$ は群となるので，これを**自己同型群**と呼ぶ．　◇

証明 [$\mathrm{Aut}(G)$ **が群**] 2 つの自己同型の合成は，G から G への準同型である：

$$\varphi(\psi(g_1 g_2)) = \varphi(\psi(g_1)\psi(g_2)) = \varphi(\psi(g_1))\varphi(\psi(g_2))\ (\varphi, \psi \in \mathrm{Aut}(G),\ g_1, g_2 \in G).$$

もちろん全単射にもなるから，$\mathrm{Aut}(G)$ は合成について閉じている．群の 3 つの条件を満たすことも明らかである．　■

例 B.2 G を群とする．各 $g \in G$ に対し，$l_g : G \to G;\ x \mapsto l_g(x) := gxg^{-1}$ は自己同型である．　◇

証明 任意に $g \in G$ をとる．l_g の逆写像は $l_{g^{-1}}$ となるから，l_g は全単射である．また，

$$l_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = l_g(x)l_g(y)\ (x, y \in G)$$

より，準同型である．　■

定義 B.5 例 B.2 の l_g を，G の**内部自己同型**という．また，各 $g, x \in G$ に対し，gxg^{-1} を g による x の**共役**という．G の内部自己同型以外の自己同型のことは，**外部自己同型**という．　◇

定義 B.6 群 G の内部自己同型全体からなる集合を $\mathrm{Inn}(G)$ とかく．$\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の部分群となるので，これを**内部自己同型群**と呼ぶ．　◇

証明 [$\mathrm{Inn}(G)$ **が** $\mathrm{Aut}(G)$ **の部分群**] G の内部自己同型を l_g $(g \in G)$ とする. 2 つの内部自己同型の合成もまた, 内部自己同型である：

$$l_{g_1}(l_{g_2}(x)) = g_1(g_2 x {g_2}^{-1}){g_1}^{-1} = (g_1 g_2)x(g_1 g_2)^{-1} = l_{g_1 g_2}(x) \ (x, g_1, g_2 \in G).$$

ゆえに $\mathrm{Inn}(G)$ は合成について閉じている. 単位元は恒等写像, l_g の逆元は $l_{g^{-1}}$ である. ■

B.3 群の作用

定義 B.7 G を群, X を集合とする. **群** G **の集合** X **への左作用**とは, 写像 $\varphi : G \times X \to X$ のうち, 以下の (1), (2) を満たすものである：

(1) $\varphi(1_G, x) = x \ (x \in X)$.

(2) $\varphi(g, \varphi(h, x)) = \varphi(gh, x) \ (g, h \in G, \ x \in X)$.

同様に, **群** G **の集合** X **への右作用**とは, 写像 $\psi : X \times G \to X$ のうち, 以下の (1), (2) を満たすものである：

(1) $\psi(x, 1_G) = x \ (x \in X)$.

(2) $\psi(\psi(x, g), h) = \psi(x, gh) \ (g, h \in G, \ x \in X)$.

群 G から集合 X への左作用 (右作用) が存在するとき, **群** G **は集合** X **に左から (右から) 作用する**という. ◇

例 B.3 $\varphi : G \times X \to X; \ (g, x) \mapsto x$ や $\psi : X \times G \to X; \ (x, g) \mapsto x$ は明かに左 (右) 作用となる. これを**自明な作用**という. ◇

特に, 群が群に作用するときのことも考えてみよう.

定理 B.1 G, X は群であるとする. このとき, 以下の (1), (2) は同値である：

(1) 群 G の " 集合 " X への左作用 $\varphi : G \times X \to X$ が存在して,

$$\varphi(g, xy) = \varphi(g, x)\varphi(g, y) \ (g \in G, \ x, y \in X)$$

が成立する (このとき, φ を群 G の群 X への左作用という).

(2) 準同型 $\phi : G \to \mathrm{Aut}(X)$ が存在する. ◇

証明

((1) ⇒ (2)) 群 G の集合 X への左作用 φ と任意の $g \in G$ をとり, $\phi_g(x) := \varphi(g, x) \ (x \in X)$ とする. まず, ϕ_g の逆写像は $\phi_{g^{-1}}$ となるから, $\phi_g : X \to X$ は全単射であって,

$$\phi_g(xy) = \varphi(g, xy) = \varphi(g, x)\varphi(g, y) = \phi_g(x)\phi_g(y) \ (x, y \in X)$$

より準同型でもあるから, $\phi_g \in \mathrm{Aut}(G)$ である. さらに,

$$\phi_{gh}(x) = \varphi(gh, x) = \varphi(g, \varphi(h, x)) = \phi_g(\phi_h(x)) \ (g, h \in G, \ x \in X)$$

となるから, $\phi : G \to \mathrm{Aut}(X); \ g \mapsto \phi_g$ は準同型である.

((2) ⇒ (1)) 準同型 $\phi : G \to \mathrm{Aut}(X); \ g \mapsto \phi_g$ をとり, $\varphi(g, x) := \phi_g(x) \ (x \in X)$ とする. すると, 上記の証明より $\varphi : G \times X \to X$ によって (1) が成立する. ■

定理 B.1 の右作用版も述べる.

定理 B.2 G, X は群であるとする. このとき, 以下の (1), (2) は同値である：

(1) 群 G の“集合”X への右作用 $\varphi : X \times G \to X$ が存在して,

$$\varphi(xy, g) = \varphi(x, g)\varphi(y, g) \ (g \in G,\ x, y \in X)$$

が成立する (このとき, φ を群 G の群 X への右作用という).

(2) 準同型 $\phi : G \to (\mathrm{Aut}(X))^{\mathrm{op}}$ が存在する. ◇

注意 B.1 定理 B.2 (2) の $(\mathrm{Aut}(X))^{\mathrm{op}}$ に関して説明する. 群 $G = (G, *)$ に対して, $g_1 *' g_2 := g_2 * g_1$ $(g_1, g_2 \in G)$ を演算とする群を群 G の**逆群**といい, $G^{\mathrm{op}} := (G, *')$ で表す. 言い換えれば, 逆群とは元の群の演算の順番を反転させて作る群のことである.

実際, 右作用 $\varphi : X \times G \to X$ に対し, $\phi_g(x) := \varphi(x, g)$ $(g \in G,\ x \in X)$ とすると,

$$\phi_{gh}(x) = \varphi(x, gh) = \varphi(\varphi(x, g), h) = \phi_h(\phi_g(x)) \ (g, h \in G,\ x \in X)$$

となり, 合成の順番が g, h に対して反転してしまうので, 準同型 ϕ の終域は $\mathrm{Aut}(X)$ の逆群としなければならない. ◇

例 B.4 G, X を群とする. 各 $g \in G$ に対し, X の恒等写像 $\mathrm{id}_X \in \mathrm{Aut}(X)$ をとると, $i : G \to \mathrm{Aut}(X);\ g \mapsto \mathrm{id}_X$ は明かに準同型である. これに対応する作用 $\iota : G \times X \to X;\ (g, x) \mapsto x$ は自明な作用である. これを群 G の群 X への自明な作用という. ◇

例 B.5 G を群とする. 各 $g \in G$ に対し, G の内部自己同型 $l_g \in \mathrm{Inn}(G)$ をとると, $l : G \to \mathrm{Aut}(G);\ g \mapsto l_g$ は準同型である. また, $r_g := l_{g^{-1}}$ に対し, $r : G \to (\mathrm{Aut}(G))^{\mathrm{op}};\ g \mapsto r_g$ は準同型である：

$$r_{g_1 g_2}(x) = (g_1 g_2)^{-1} x (g_1 g_2) = {g_2}^{-1}({g_1}^{-1} x g_1) g_2 = r_{g_2}(r_{g_1}(x)) \ (x, g_1, g_2 \in G).$$

すなわち, l, r はそれぞれ群 G の群 G への左作用 (右作用) を与える. ◇

C 半直積

C.1 半直積の定義

まずは群の直積を定義する.

定義 C.1 G, H を群とする. 直積集合 $G \times H$ は,

$$(g_1, h_1)(g_2, h_2) := (g_1 g_2, h_1 h_2) \ ((g_1, h_1), (g_2, h_2) \in G \times H)$$

で定められる演算により群となる. これを G と H の**直積群**といい, $G \times H$ とかく. ◇

次に, 半直積という概念を定義する. 半“直積”というからには直積群の一般化になっているのであるが, その詳細は後に述べる. 内部半直積から定義しよう.

定義 C.2 群 G とその部分群 N, H が, 以下の (1)〜(3) を満たすとする：

(1) $N \triangleleft G$.

(2) $NH = G$[*14].

[*14] $NH := \{nh \mid n \in N,\ h \in H\}$.

(3) $N \cap H = \{1_G\}$.

このとき, G を N と H の**内部半直積**といい, $N \rtimes H$ で表す. $\diamond$

内部半直積では N, H が共通の群 G の部分群である必要があったが, これに対し外部半直積は一般の群 N, H に対して定義するものである.

定義 C.3 群 N, H に対し, 準同型 $\phi : H \to \mathrm{Aut}(N)$ が与えられているとする[*15]. このとき, 直積集合 $N \times H$ は

$$(n_1, h_1)(n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2) \ ((n_1, h_1), (n_2, h_2) \in N \times H)$$

で定められる演算により群となる (ただし, $\phi_{h_1} \coloneqq \phi(h_1)$. この表記はしばらく用いる). これを N と H の**外部半直積**といい, $N \rtimes_\phi H$ で表す. $\diamond$

証明 [**外部半直積は群**] [*16] 任意に $(n, h) \in N \times H$ をとると,

$$\begin{aligned}(1_N, 1_H)(n, h) &= (1_N\phi_{1_H}(n), 1_Hh) = (1_Nn, h) = (n, h),\\ (n, h)(1_N, 1_H) &= (n\phi_h(1_N), h1_H) = (n1_N, h) = (n, h)\end{aligned}$$

より, $(1_N, 1_H) \in N \times H$ は単位元であり,

$$\begin{aligned}(\phi_{h^{-1}}(n^{-1}), h^{-1})(n, h) &= (\phi_{h^{-1}}(n^{-1})\phi_{h^{-1}}(n), h^{-1}h) = (\phi_{h^{-1}}(n^{-1}n), 1_H) = (1_N, 1_H),\\ (n, h)(\phi_{h^{-1}}(n^{-1}), h^{-1}) &= (n\phi_h(\phi_{h^{-1}}(n^{-1})), hh^{-1}) = (n\phi_{hh^{-1}}(n^{-1}), 1_H) = (1_N, 1_H)\end{aligned}$$

より, $(\phi_{h^{-1}}(n^{-1}), h^{-1}) \in N \times H$ は (n, h) の逆元である.

また, 任意に $(n_1, h_1), (n_2, h_2), (n_3, h_3) \in N \times H$ をとると,

$$\begin{aligned}((n_1, h_1)(n_2, h_2))(n_3, h_3) &= (n_1\phi_{h_1}(n_2), h_1h_2)(n_3, h_3)\\ &= (n_1\phi_{h_1}(n_2)\phi_{h_1h_2}(n_3), (h_1h_2)h_3)\\ &= (n_1\phi_{h_1}(n_2\phi_{h_2}(n_3)), h_1(h_2h_3))\\ &= (n_1, h_1)(n_2\phi_{h_2}(n_3), h_2h_3)\\ &= (n_1, h_1)((n_2, h_2)(n_3, h_3))\end{aligned}$$

より, 結合則も成り立つ. ■

注意 C.1 与えられた準同型 $\phi : H \to (\mathrm{Aut}(N))^{\mathrm{op}}$ に対して, 直積集合 $H \times N$ 上の演算を

$$(h_1, n_1)(h_2, n_2) = (h_1h_2, \phi_{h_2}(n_1)n_2) \ ((h_1, n_1), (h_2, n_2) \in H \times N)$$

で定めても群となる. このとき, 群 $H \times N$ を $H \ltimes_\phi N$ で表す[*17]. $\diamond$

注意 C.2 内部半直積 $N \rtimes H$ は集合として $N \times H$ と等しくはないが, 外部半直積 $N \rtimes_\phi H$ は集合として $N \times H$ と等しい. $\diamond$

C.2 内部半直積と外部半直積の関係

一見全く異なる定義に見える内部半直積と外部半直積であるが, 以下に示すように, 外部半直積は自身の 2 つの部分群の内部半直積となる.

[*15] 定理 B.1 より, 群 H が群 N に左から作用していることと同値である.

[*16] 証明の本質的な部分は本文中の定理 4.3 の証明で済ませてあるが, 改めてここにも示しておく. なお, 本文中では H が N に右から作用する場合であったが, ここに示すのは左作用の場合であることに注意 (注意 C.1 参照).

[*17] 定義 C.3 の演算の式の成分を入れ替えただけでももちろん群になるので, それを $H \ltimes_\phi N$ とかくこともある.

定理 C.1 群 N, H に対し, 準同型 $\phi : H \to \mathrm{Aut}(N)$ が与えられているとき,

$$N' \coloneqq \{(n, 1_H) \mid n \in N\},\ H' \coloneqq \{(1_N, h) \mid h \in H\}$$

とおくと, $N \rtimes_\phi H = N' \rtimes H'$ が成り立つ. $\diamond$

証明 まず, N', H' は $N \rtimes_\phi H$ の部分群である：

$$\begin{aligned}
&(1_N, 1_H) \in N', H' \ (\phi_{1_H{}^{-1}}(n^{-1}), 1_H{}^{-1}) = (n^{-1}, 1_H) \in N' \ (n \in N),\\
&(n_1, 1_H)(n_2, 1_H) = (n_1\phi_{1_H}(n_2), 1_H) = (n_1 n_2, 1_H) \in N' \ (n_1, n_2 \in N),\\
&(\phi_{h^{-1}}(1_N), h^{-1}) = (1_N, h^{-1}) \in N' \ (h \in H),\\
&(1_N, h_1)(1_N, h_2) = (1_N\phi_{h_1}(1_N), h_1 h_2) = (1_N, h_1 h_2) \in H' \ (h_1, h_2 \in H).
\end{aligned}$$

(演算の成分の対応を見れば, ついでに $N' \cong N,\ H' \cong H$ も分かる) ここで, N', H' が定義 C.2 の条件を満たすことを確認しよう. (1) について, 任意の $(n, h) \in N \rtimes_\phi H$ および $(n', 1_H) \in N'$ に対し,

$$\begin{aligned}
(n, h)(n', 1_H)(\phi_{h^{-1}}(n^{-1}), h^{-1}) &= (n\phi_h(n'), h)(\phi_{h^{-1}}(n^{-1}), h^{-1})\\
&= (n\phi_h(n')\phi_h(\phi_{h^{-1}}(n^{-1})), hh^{-1})\\
&= (n\phi_h(n')n^{-1}, 1_H) \in N'.
\end{aligned}$$

よって, $N' \triangleleft N \rtimes H$ となる. また, (2) は,

$$\begin{aligned}
N'H' &= \{(n, 1_H)(1_N, h) \mid n \in N, h \in H\}\\
&= \{(n\phi_{1_H}(1_N), h) \mid n \in N, h \in H\}\\
&= \{(n, h) \mid n \in N, h \in H\}\\
&= N \rtimes_\phi H
\end{aligned}$$

より成立する. (3) についても, $N' \cap H' = \{(1_N, 1_H)\} = \{1_{N \rtimes_\phi H}\}$ より成立する. ■

逆に, 内部半直積は内部自己同型に対応させる作用による外部半直積と同型である.

定理 C.2 群 N, H の内部半直積 $N \rtimes H$ が定義されるとき, 準同型 $\phi : H \to \mathrm{Aut}(N)$ が存在して, $N \rtimes H \cong N \rtimes_\phi H$ が成り立つ. $\diamond$

証明 定義 C.2 (1) より $N \triangleleft N \rtimes H$ であるから, 写像 $\Phi : N \rtimes H \to \mathrm{Aut}(N);\ g \mapsto l_g$ が定まる. 例 B.5 より Φ は準同型だから, $\phi \coloneqq \Phi|_H$ とおくと準同型 $\phi : H \to \mathrm{Aut}(N)$ によって外部半直積 $N \rtimes_\phi H$ が定義できる. いま, $\iota : N \rtimes H \to N \rtimes_\phi H;\ nh \mapsto (n, h)$ が同型であることを示そう.

まず, 任意に $n_1h_1, n_2h_2 \in N \rtimes H$ をとる. $n_1h_1 = n_2h_2$ とすると, ${n_2}^{-1}n_1 = h_2{h_1}^{-1} \in N \cap H$ であり, 定義 C.2 (3) より $n_1 = n_2$ かつ $h_1 = h_2$ となるから, ι は well-defined であり[*18],

$$\begin{aligned}
\iota((n_1h_1)(n_2h_2)) &= \iota((n_1(h_1n_2{h_1}^{-1}))(h_1h_2))\\
&= \iota((n_1l_{h_1}(n_2))(h_1h_2))\\
&= (n_1l_{h_1}(n_2), h_1h_2)\\
&= (n_1, h_1)(n_2, h_2)\\
&= \iota(n_1h_1)\iota(n_2h_2)
\end{aligned}$$

[*18] 一般に, 写像 $f : A \to B$ は任意の $a_1, a_2 \in A$ について $a_1 = a_2 \ \Rightarrow\ f(a_1) = f(a_2)$ を満たさなければならない (このとき, 写像 f は **well-defined** であるという). 今回の場合, $n_1h_1 = n_2h_2 \ \Rightarrow\ (n_1, h_1) = (n_2, h_2)$ は全くもって自明ではない. なお, 逆は自明なので ι^{-1} を用いるとこの確認は不要となるが, その場合単射の確認に定義 C.2 (3) が必要となる (そのように示している文献が多い [5], [6], [8]).

より準同型となる．また, 定義 C.2 (2) より ι は全射となる．さらに, $\iota(n_1h_1) = \iota(n_2h_2)$ とすると, $(n_1, h_1) = (n_2, h_2)$ から $n_1h_1 = n_2h_2$ なので ι は単射である．以上より ι は同型なので, $N \rtimes H \cong N \rtimes_\phi H$ が従う． ■

以上より, 内部半直積と外部半直積の定義は本質的に等価である.

C.3 半直積と直積の関係

最後に, 半直積が直積群の一般化になっていることの確認をしよう．唐突に登場した内部半直積の定義条件は, 実は以下の命題から来たものである.

命題 C.1 群 G とその部分群 N, H が, 以下の (1)〜(3) を満たすとする：

(1) $N, H \triangleleft G$.

(2) $NH = G$.

(3) $N \cap H = \{1_G\}$.

このとき, $G \cong N \times H$ である． ◇

証明 $\iota : G \to N \times H;\ nh \mapsto (n, h)$ が同型であることを示そう．定理 C.2 の証明と同様にして, ι が well-defined で全単射であることまでは分かる．準同型については, 任意の $n_1h_1, n_2h_2 \in N \times H$ をとり, (1) から ${n_2}^{-1}h_1n_2{h_1}^{-1} \in N \cap H$ であることに注意して,

$$\begin{aligned}
\iota((n_1h_1)(n_2h_2)) &= \iota((n_1n_2)({n_2}^{-1}h_1n_2{h_1}^{-1})(h_1h_2)) \\
&= \iota((n_1n_2)(h_1h_2)) \ (\because (3)) \\
&= (n_1n_2, h_1h_2) \\
&= (n_1, h_1)(n_2, h_2) \\
&= \iota(n_1h_1)\iota(n_2h_2)
\end{aligned}$$

より従う．以上より $G \cong N \times H$ である． ■

注意 C.3 命題 C.1 の G を N と H の**内部直積**と呼ぶことがある (これに対して直積群のことを**外部直積**と呼ぶ)． ◇

すなわち, 内部直積の一般化が内部半直積となっているのである．そして, 外部直積 (直積群) の一般化が外部半直積であることはすぐに分かる.

命題 C.2 群 N, H に対し, N の恒等写像 id_N 対応させる準同型 $i : H \to \mathrm{Aut}(N);\ h \mapsto \mathrm{id}_N$ が与えられているとき, $N \rtimes_i H = N \rtimes H$ である． ◇

証明 $(n_1, h_1)(n_2, h_2) = (n_1 i_{h_1}(n_2), h_1h_2) = (n_1n_2, h_1h_2)$ $((n_1, h_1), (n_2, h_2) \in N \times H)$. ■

D その他の道具 (交換子, supp)

D.1 交換子について

定義 D.1 G を群とするとき, $g, h \in G$ に対し $[g, h]$ を

$$[g, h] \coloneqq h^{-1}g^{-1}hg$$

で定義し, これを g と h の**交換子**という． ◇

注意 D.1 $[g,h] \coloneqq ghg^{-1}h^{-1}$ と定義されていることもある. ある集合に左から作用している群の元に対して交換子を用いる場合は, 定義 D.1 の方が分かりやすい, と思われる. $\diamond$

注意 D.2 もし g と h が可換 (すなわち $gh = hg$) なら, $[g,h] = 1_G$ である. この意味で, 交換子はある 2 つの元が交換可能かどうかを測る指標ということもできる. $\diamond$

例 D.1 $[g,h]^{-1} = g^{-1}h^{-1}gh = [h,g]$ である. $\diamond$

例 D.2 任意の $\sigma, \tau \in S_n$ に対し, $[\sigma,\tau]$ は偶置換である. 実際, 例 B.1 より sgn は準同型なので, $\mathrm{sgn}(\sigma) = (-1)^N$, $\mathrm{sgn}(\tau) = (-1)^M$ であるとすると,

$$\mathrm{sgn}([\sigma,\tau]) = \mathrm{sgn}(\tau^{-1})\mathrm{sgn}(\sigma^{-1})\mathrm{sgn}(\tau)\mathrm{sgn}(\sigma) = (-1)^{2N}(-1)^{2M} = 1 \quad \diamond$$

D.2 supp について

定義 D.2 φ を群 G から集合 X への左作用とする. このとき, $g \in G$ に対し $\mathrm{supp}(g)$ を

$$\mathrm{supp}(g) \coloneqq \{x \in X \mid \varphi(g,x) \neq x\}$$

で定義し, これを g の**台**という. 右作用の場合についても同様に定義する. $\diamond$

注意 D.3 解析学では, 集合 X 上で定義された関数 f に対して $\mathrm{supp}(f) \coloneqq \{x \in X \mid f(x) \neq 0\}$ で定義される. $\diamond$

命題 D.1 φ を群 G から集合 X への左作用とするとき, 任意の $g \in G$ に対して以下の (1), (2) が成り立つ.

(1) $\forall x \in \mathrm{supp}(g), \varphi(g,x) \in \mathrm{supp}(g)$.

(2) $\mathrm{supp}(g) = \mathrm{supp}(g^{-1})$. $\diamond$

証明 任意に g をとる.

(1) 任意の $x \in \mathrm{supp}(g)$ について, $\varphi(g,x) \neq x$ より $\varphi(g,\varphi(g,x)) \neq \varphi(g,x)$ であるから, $\varphi(g,x) \in \mathrm{supp}(g)$.

(2) 任意の $x \in \mathrm{supp}(g)$ について, $\varphi(g,x) \neq x$ より $\varphi(g^{-1},\varphi(g,x)) \neq \varphi(g^{-1},x)$ であるが, 一方 $\varphi(g^{-1},\varphi(g,x)) = \varphi(1_G,x) = x$ であるから, $\varphi(g^{-1},x) \neq x$. よって, $x \in \mathrm{supp}(g^{-1})$. 同様にして, 任意の $x' \in \mathrm{supp}(g^{-1})$ について $x' \in \mathrm{supp}(g)$. ゆえに, $\mathrm{supp}(g) = \mathrm{supp}(g^{-1})$. ■