2018 年 6 月 23 日　数理ウェーブ（於：名古屋大学）

ルービックキューブと数学

名古屋大学大学院多元数理科学研究科
中島秀斗

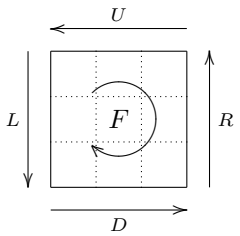
1　はじめに

ルービックキューブという立体パズルがある．このパズルは，ハンガリーの建築学者ルビク・エルネー (Rubik Ernö) により，1974 年に考案されたものである．ルービックキューブは，単純なパズルとしてはもちろん，バラバラの状態から如何に速く揃えられるかを競ういわゆるスピードキュービングなど，生まれて 40 年以上経った今でも広く親しまれている．実はルービックキューブは，数学的にも非常に興味深い研究対象である．たとえば「ルービックキューブの配置は全部で何通りあるか」という問題や，「どのような配置からでも，高々 N 手で各面を揃えられる」という最小の数 N を決定する問題[*1]には，数理的な手法で解決できるのだ．その背景には，現代数学において不可欠な「群」というものが隠れている．今日は「同じ操作を繰り返すとどうなるか」という素朴な問題を出発点として，少しだけその群論に触れてみよう．

2　ルービックキューブ

ルービックキューブを手に持って操作するときは，どこが上になっているかなどはあまり気にしないが，紙に書いて伝えるときにはそれだと不都合である．この小論では，底面と手前の面を固定しておいて（例えば青が下，赤が手前，など），ルービックキューブの基本操作を次のように記述することにする．

F (Front) : 前面を時計回りに回す．
R (Right) : 右面を時計回りに回す．
L (Left)　: 左面を時計回りに回す．
B (Back) : 裏面を時計回りに回す．
U (Up)　: 上面を時計回りに回す．
D (Down): 底面を時計回りに回す．



以下では，操作といえば上の基本操作を有限回組み合わせたもの（たとえば $FURL$ など）を指すこととする．また，たとえば F^2 と書けば，F を 2 回繰り返す操作，すなわち前面を 180 度回転させる操作を表すことにする．明らかに基本操作を 4 回繰り返せば元の状態に戻る．これより特に，たとえば F を反時計回りに回転させる操作 F^{-1} は，F を 3 回繰り返したもの F^3 と同じになる．さて，一般に同じ操作を何度も繰り返したときにどういう事が起こるのだろうか．次の操作で実験してみよう．

演習問題 2.1　次の操作を繰り返し実行せよ．何が起こるだろうか．回数も数えておくこと．

(1)　$FU^{-1}F^{-1}U$　　(2)　FU^{-1}

この問題より，例えば次のような問題が自然に提起される．

- どのような操作も，適当な回数繰り返せば元の状態に戻るか?
- 与えられた回数，たとえば丁度 17 回だけ繰り返して元の状態に戻るような操作は存在するか？

群論は，この問題に答えを教えてくれる．

[*1] 神の数字 (God's number) という素敵な名前がついている．

3　群とその例

まずはいきなり群の定義を書いてみよう．

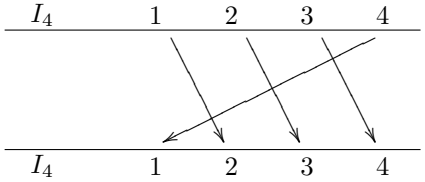
定義 3.1　集合 G が**群**であるとは，G 上に演算 $G \times G \ni (g,h) \mapsto gh \in G$ が定義されていて[*2]，次の三条件を満たすことをいう．
(1) 結合法則を満たす：任意の三元 $g,h,k \in G$ に対して $(gh)k = g(hk)$;
(2) 単位元 e の存在：任意の $g \in G$ に対して $ge = eg = g$;
(3) 逆元の存在：任意の $g \in G$ に対して $gh = hg = e$ となる $h \in G$ がある（g^{-1} と表す）．

例えば，① 整数全体の集合と足し算の組，② 0 以外の実数の集合と掛け算の組，などは群である．しかし ③ 自然数の集合と足し算の組，は群にはならない．それは，単位元も逆元も自然数の中には存在していないからである．つまり群とは，元の集合からはみ出ることなしに，自由に演算ができる集合のことである．

注意 3.2　群はまた，図形の対称性としても説明される．たとえば正方形□について考える．中心を軸として 45 度だけ回転させると◇となり，さらに 45 度だけ回転させると再び元の形□に戻る．つまり，90 度回転させると，見た目上は全く動いていないように見える (もちろん，各頂点は動いている)．また，上下左右の折返しや対角線を軸とした折返しでも，見た目上は動かない．このような図形の形を変えないような変換の全体というものも群になり，その群の大きさで対称性の高さが表現される．例えば円 ◯ は非常に高い対称性を持つが，♠ は左右反転程度の対称性しか持たない．

§3.1 対称群．群の重要な例として，対称群 S_n がある．これは，n 文字の入れ替えからなる集合であり，順列の組み合わせを考えると，その全体は $n!$ 個になることが分かる．S_n の元のことを置換という．

例 3.3　$n = 4$ のとき．



$$\begin{cases} \sigma(1) = 4 \\ \sigma(2) = 1 \\ \sigma(3) = 2 \\ \sigma(4) = 3 \end{cases} \quad \text{とすれば，} \sigma \in S_4.$$

これを $\sigma = \begin{pmatrix} 1&2&3&4 \\ \downarrow&\downarrow&\downarrow&\downarrow \\ 2&3&4&1 \end{pmatrix}$ と表す (普通は矢印は書かない)．

$1,2,\ldots,n$ のうち，$k_1,k_2,\ldots,k_r$ 以外は動かさずに，$k_1 \to k_2$, $k_2 \to k_3$, …, $k_{r-1} \to k_r$, $k_r \to k_1$ と順にずらす置換のこと巡回置換という．これを $(k_1\, k_2\, \ldots\, k_r)$ と表す．例 3.3 の σ は巡回置換であり，$\sigma = (1\,2\,3\,4)$ である．また，二つの $\sigma,\tau \in S_n$ の積 $\sigma \circ \tau \in S_n$ は次で定義される:

$$(\sigma \circ \tau)(i) := \sigma(\tau(i)) \quad (i = 1,\ldots,n).$$

単位元は $e = \begin{pmatrix} 1&2&\cdots&n \\ \downarrow&\downarrow&\cdots&\downarrow \\ 1&2&\cdots&n \end{pmatrix}$ という置換であり，置換 $\begin{pmatrix} 1&2&\cdots&n \\ \downarrow&\downarrow&\cdots&\downarrow \\ s_1&s_2&\cdots&s_n \end{pmatrix}$ の逆元は $\begin{pmatrix} s_1&s_2&\cdots&s_n \\ \downarrow&\downarrow&\cdots&\downarrow \\ 1&2&\cdots&n \end{pmatrix}$ となる[*3]．

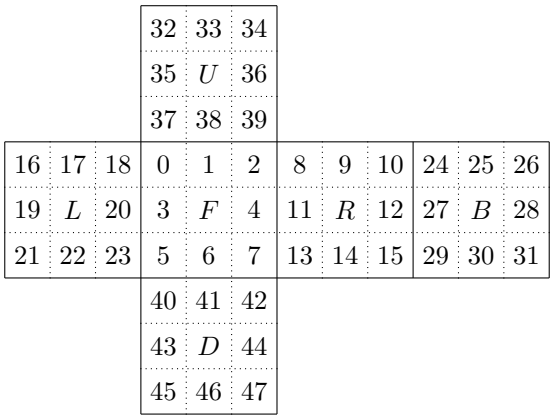
注意 3.4　右にある τ から先に計算することに注意．例えば，例 3.3 の σ と $\tau = \begin{pmatrix} 1&2&3&4 \\ \downarrow&\downarrow&\downarrow&\downarrow \\ 2&1&4&3 \end{pmatrix}$ との積は，

$$\begin{array}{ccccc} & \tau & & \sigma & \\ 1 & \to & 2 & \to & 3 \\ 2 & \to & 1 & \to & 2 \\ 3 & \to & 4 & \to & 1 \\ 4 & \to & 3 & \to & 4 \end{array} \quad \text{より} \quad \sigma \circ \tau = \begin{pmatrix} 1&2&3&4 \\ \downarrow&\downarrow&\downarrow&\downarrow \\ 3&2&1&4 \end{pmatrix} = (1\,3); \quad \text{同様に } \tau \circ \sigma = (2\,4).$$

[*2] 普通は積と呼ばれる．さらに可換 (任意の $g,h \in G$ に対して $gh = hg$) であるときは，和と呼ばれることも多い．
[*3] 大事なのは上下の組なので，このように列を入れ替えて書くこともできる．

4　ルービックキューブの群

ルービックキューブは $9 \times 6 = 54$ 個のマスがあるが，そのうち中央に配置されている 6 個のマスは動かないとしているので，$54 - 6 = 48$ 個のマスが入れ替わっていることになる．つまり，ルービックキューブは S_{48} (の部分群) と思うことができる．そこで，各マスを次のように番号付けることにする[*4]．



このように番号を付ければ，各基本操作 F, R, L, B, U, D は次のような置換と対応することになる．

$$
\begin{aligned}
F &= (\ 0\ \ 5\ \ 7\ \ 2\ )(\ 1\ \ 3\ \ 6\ \ 4\ )(\ 8\ 37\ 23\ 42\ )(\ 11\ 38\ 20\ 41\ )(\ 13\ 39\ 18\ 40\ )\\
R &= (\ 2\ 42\ 29\ 34\ )(\ 4\ 44\ 27\ 36\ )(\ 7\ 47\ 24\ 39\ )(\ 8\ 13\ 15\ 10\ )(\ 9\ 11\ 14\ 12\ )\\
L &= (\ 0\ 32\ 31\ 40\ )(\ 3\ 35\ 28\ 43\ )(\ 5\ 37\ 26\ 45\ )(\ 16\ 21\ 23\ 18\ )(\ 17\ 19\ 22\ 20\ )\\
B &= (\ 10\ 47\ 21\ 32\ )(\ 12\ 46\ 19\ 33\ )(\ 15\ 45\ 16\ 34\ )(\ 24\ 29\ 31\ 26\ )(\ 25\ 27\ 30\ 28\ )\\
U &= (\ 0\ \ 8\ 24\ 16\ )(\ 1\ \ 9\ 25\ 17\ )(\ 2\ 10\ 26\ 18\ )(\ 32\ 37\ 39\ 34\ )(\ 33\ 35\ 38\ 36\ )\\
D &= (\ 5\ 21\ 29\ 13\ )(\ 6\ 22\ 30\ 14\ )(\ 7\ 23\ 31\ 15\ )(\ 40\ 45\ 47\ 42\ )(\ 41\ 43\ 46\ 44\ )
\end{aligned}
$$

ルービックキューブは，これら 6 つの操作を適当に繰り返すことにより得られる．このことを，ルービックキューブの群 G_{rub} は F, R, L, B, U, D で生成されるという．そのような群の位数 (要素の数) は，コンピュータを用いると，簡単に計算することができる．もちろん，理論的に導くことも可能である[*5]．

定理 4.1　群 G_{rub} の位数は，$43252003274489856000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$ である[*6]．

位数が分かったことにより，はじめに述べた問題に解答を与えることができる．まず，「同じ操作を繰り返す」ということを，群の言葉で言い換えよう．考えている操作に対応する群の元を g と書く．このとき，操作を繰り返すということは g を何度も掛けていくこと，すなわち $e = g^0, g^1, g^2, \ldots, g^k, \ldots$ を考えることと対応する．ここで，今考えている群 G_{rub} は有限集合であるので，

相異なる番号 j, k で $g^j = g^k$ となるものが存在する

ことがわかる[*7]．$j < k$ とすれば，等式の両辺に g^j の逆元 g^{-j} をかけることによって $g^{k-j} = e$ (単位元) を得る．すなわち「どのような操作も適切な回数だけ繰り返すことによって元に戻る」ということがわかる．さて，$H = \{g^k;\, k = 0, 1, 2, \ldots\}$ とすると，これは先程の議論により有限集合であり，さらに G_{rub} の部分群となる．部分群の位数について，次のことが成り立つことが知られている．

[*4] 番号を 0 からにしているのは，javascript の配列が 0 から始まるという理由である．そのメリットの一つとして，番号を 8 で割った商によって，どの面に配置されている番号かを判別可能になるということがある．

[*5] 興味のある方は，参考文献 [2] を参照してください．

[*6] 4325 京 2003 兆 2744 億 8985 万 6000.

[*7] もしそのような番号の組が存在しなければ，集合 G_{rub} は無限集合となってしまう．このような論法は鳩の巣原理と呼ばれる．

定理 4.2　有限群 G の部分群 H があったとき，H の位数 $|H|$ は，G の位数 $|G|$ の約数になる．

この定理とルービックキューブ群の位数は 17 の因子を持たないことにより，ルービックキューブの操作の中で「ちょうど 17 回繰り返すと元に戻る操作」は存在しないことが分かる[*8]．一方で，次の定理もある．

定理 4.3　有限群 G の位数が素数 p で割り切れるならば，G は必ず位数 p の元を持つ．

この定理は**シローの定理**という大定理からの帰結である．シローの定理は有限群論の中でも応用の幅が広くとても美しい定理の一つである．これよりルービックキューブ群 G_{rub} には位数 5, 7, 11 の元が存在することがわかるが，そのベキ，たとえば 5^4 などの位数を持つ元が存在するかどうかまではわからない．

演習問題 4.4　次の操作の位数を求めよ．

$$(1)\quad R^{-1}URU \qquad (2)\quad (D^2R)^2(U^2L)^2 \qquad (3)\quad (R^{-1}UF^{-1}L)^3$$

5　おまけ

この講演ではルービックキューブの操作の位数について扱ったが，それ以外にも興味深い話題があるので，それについて簡単に紹介する．

1. **ルービックキューブを解くアルゴリズム**
   底面から順に色を揃えていく LBL 法（Layer by Layer 法）が一般的である．まず底面を十字に揃える．次にコーナーキューブを揃え，そして二段目のエッジキューブも揃える[*9]．ここまでは覚える手順はほとんどなく，少し勉強をすればすぐに揃えられるようになる．最後のステップは（文章で説明するのは）大変なので割愛させていただく．ここで重要な役割を果たすのは，コーナーキューブあるいはエッジキューブを順に置換する位数 3 の操作である．私が覚えている手順は 5,6 通り程度であるが，それでも十分である．
2. **最短手順 (God's number)**
   「与えられた任意の配置から全面すべて揃えるまでに必要となる最短手順は何手か」という問題は，多くの研究者によって研究され，最終的には Morley Davidson を中心とした数学者やプログラマー等によるグループ[*10]によって，それは 20 手であることが証明された．そのことについては，ウェブページ (http://www.cube20.org) に詳しく記述されている（ただし英語）．しかし，それがどのようなアルゴリズムなのか (或いは存在するのか) ということは分かっていない．
3. **スピードキューブ**
   バラバラの状態から，全面が揃った状態に戻す時間を競う競技をスピードキューブという．現在の世界記録はなんと，4.59 秒であり，平均[*11]の世界記録でも僅か 6.43 秒というから驚きである．また，ロボットが 0.38 秒で揃える様子も，動画サイトで見ることができる．これ以上速くするのは物理的に難しいらしく，いろいろ試行錯誤がなされているようである．動画サイトには失敗している動画もあるので，興味のある方はそちらも視聴されてみてはいかがだろうか．

[*8] 存在すると仮定すると，対応する元から生成される群を考えれば，その位数は 17 になるが，それはこの定理と矛盾している．
[*9] コーナーキューブは「角」，エッジキューブは「辺」．
[*10] Tomas Rokicki, Herbert Kociemba, Morley Davidson, John Dethridge によるグループ．
[*11] 5 回計測して、その中で一番良いタイムと悪いタイムを除いたものの平均をとる．

4. **素数位数の操作の探索**

   素数位数 (特に 5, 7, 11) の操作を探すのには，p-Sylow 群をコンピュータで計算し，ルービックキューブの操作に書き直すという手順を踏む（参考文献 [3] 参照）．しかし，与えられた自然数に対して，その位数を持つ操作を探すことは難しい．ただし，ルービックキューブの操作の位数の最大値はすでに求められている．操作 $RF^2B^{-1}UB^{-1}$ がその最大位数を与えるので，興味ある方は実際に求めてみては如何だろう (文献 [4] を参照のこと)．

ルービックキューブの亜種として，ポケットキューブ ($2 \times 2 \times 2$) やルービックキューブリベンジ ($4 \times 4 \times 4$)，あるいはプロフェッサーキューブ ($5 \times 5 \times 5$) というものもある．当然ながら辺の数が増えるほどに難しくなるが，それでもやはり群論の枠組みで考えることが可能である．

参考文献

[1] 志賀浩二，「群論への 30 講」，朝倉書店，1989.

[2] 島内剛一，「ルービック・キューブと数学パズル」，亀書房，2008.

[3] 藤本光史・泊昌孝，「数式処理を用いたルービックキューブの素数位数操作の探求」，MI lecture note series. **49**, pp. 69–77, 2013.

[4] D. Singmaster, Notes on Rubik's Magic Cube, Enslow Pub Inc, 1981.

今回の講演は，主に文献 [3] を参考にした．特に数式処理を用いたルービックキューブ群の扱い方も丁寧に書いてあるので，それを参考にして，プロフェッサーキューブやルービックリベンジなどに挑戦することも可能であろう．この文献はインターネットから入手可能である．書籍 [2] はルービックキューブについて数学の視点から扱った本である．ルービックキューブ群の位数についても理論的に導出しているので，興味のある方はご一読ください．書籍 [4] はルービックキューブ群の元における最大位数を決定している．ただし英語である．群論に関する入門書としては書籍 [1] を挙げておく．以下は数理ウェーブではお馴染みの伊師英之氏による書評の抜粋である[*12]:

> “（前略）その後，評者が群に少しずつ親しみを感じるようになったのは，そこに空間の回転のような「動き」を感じたからでした。本書『群論への 30 講』は，まさにその群の動的なイメージを大切にしたところに特色のある入門書です。（中略）語りかけるような文体の中に含蓄のある言葉が散りばめられていて読むたびに新しい味わいがあり，本書は読み物としても非常に魅力的です。群とは何かが知りたい全ての人に薦めます。”

[*12] 『数学セミナー　2007 年 8 月号』（日本評論社）の「特集：数セミ・ブックガイドＡＢＣ」欄より．