パズルと数学

— 対称群の世界 —

庄司 俊明

名古屋大学大学院多元数理科学研究科*

講義のタイトルは「パズルと数学」としましたが, ここで扱う対象はパズルというよりは一人ゲームです. 「ゲームと数学」とすると, どうしても２人以上でやる対戦型ゲームに関するゲームの理論を連想してしまうので, あえてこの題名にしました。(映画「ビューティフルマインド」でジョン・ナッシュの研究していたのがゲームの理論です). この講義では, 「あみだくじ」,「１５ゲーム」,「ルービック・キューブ」を取り上げます. これらのゲームには, ある物（数字, 駒, 立方体など）を簡単なルールに基づいて, くりかえし置き換えていくという共通点があります. この置き換えるという操作 (略して**置換**という) を数学的に調べるのが群論, 特に対称群の理論です.

講義では, 「対称群の眼鏡」を通してゲームを見直すことにより, 身近かにあって普段数学とは無縁なものと思われているゲームの, 隠された数学的構造を調べていきます. ひとつひとつのゲームの背後に対称群やその親類の群がひそんでいて, 目には見えないけれども実はこれらの群がゲームの枠組みを完全にコントロールしている, ということを理解して頂けたらと思います. (必ずしもゲームの実際的解法をやるわけではありません. 念のため). この講義に予備知識は全く必要ありませんが, 高校までとは毛色の違った数学なので慣れないと難しいかも知れません. 是非自分の手でゲームを動かして抽象的な理論と現実のゲームの共同作業を楽しんでみて下さい.

1. あみだくじ

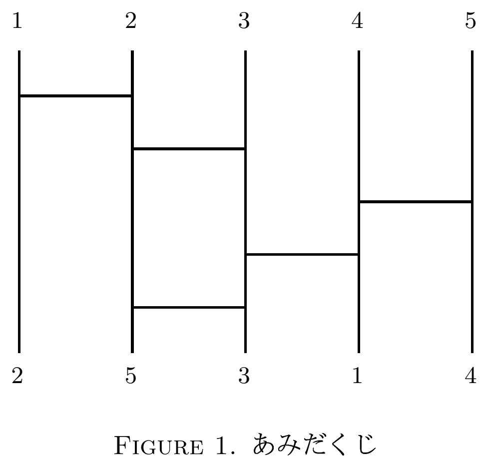


Figure 1. あみだくじ

あみだくじは誰でも知っているように縦線を何本か引いて, 横線でつないだものである. ここでは後の都合上, 横線の位置は全て高さが違うようにしておく (上の図参照). 又, 通常当りくじをひと

*より詳しい解説を私のホームページ http://www.math.nagoya-u.ac.jp/∼shoji に載せる予定です

つ決めておくが, その代りに図のように縦線の上端に数字を順番に並べ, 下端にあみだを辿っていって得られる数字を書く. 結果として文字 (以下では数字を単に文字として扱う) $\{1,2,3,4,5\}$ の列が文字 $\{2,5,3,1,4\}$ の列に変ったことになる. この操作を

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$$

と書き表す. これだけだと普通の順列と何も変らないが, あみだくじの大事な所は, この下側の列が上側の列からあみだの操作に従って数字をひとつひとつ入れ換えて行くことによって得られるという点にある. 下図からも分かるように数字の入れ換えがあみだの横線に対応していることに注意しよう.

スタート	1		2		3		4		5
1 回目	1	$\leftrightarrow$	2		3		4		5
2 回目	2		1	$\leftrightarrow$	3		4		5
3 回目	2		3		1		4	$\leftrightarrow$	5
4 回目	2		3		1	$\leftrightarrow$	5		4
5 回目	2		3	$\leftrightarrow$	5		1		4
ゴール	2		5		3		1		4

Table 1. あみだくじによる数字の置換

ここでは並べられた数字が問題なのではなく, どのように並べ変えるかという **操作** が重要なのである. 実はこの点に考えかたの大きな飛躍がある. 並べられた数字は紙の上にあって静止しているが, 我々はあみだくじのように数字を移していくという動作そのものに興味を持つ. その意味で, w を

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 2 & 5 & 1 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$$

とも表わす. w は並べ方ではなく, 1 を 2 に移し, 2 を 5 に移し, 3 を 3 に移し, 4 を 1 に移すという操作そのものを意味する. w を $\{1, 2, 3, 4, 5\}$ の置換という.

一般に n 個の文字 $\{1,2,\ldots,n\}$ の置換を考え, その置換全体の集合を S_n と表わす. n 文字の置換は $\{1,2,\ldots,n\}$ の順列の個数だけあるので, S_n は $n!$ 個の元からなる. S_n の元の間に置換を続けて行うことにより**積**を定義する. 例えば $n=3$ とすると

$$w = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad w' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \Longrightarrow \quad ww' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

により, w と w' の積 ww' が定まる. (右から左へ, w' により 1 が 2 に行き, 次いで w により 2 が 3 に行く. そこで, ww' により 1 が 3 に移る. 他の数字も同様の規則で定まる.

S_n の元

$$w_0 = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

を**恒等置換**という. w_0 は要するに何も動かさないということなので, 全ての元 $w \in S_n$ に対して $ww_0 = w_0w = w$ が成立する. また $w \in S_n$ が与えられると, $ww^{-1} = w^{-1}w = w_0$ となる元 w^{-1} が

唯ひとつ 定まる. w^{-1} を w の**逆置換**という. 例えば $n=3$ のとき

$$w = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \Longrightarrow \quad w^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

これらの性質は, S_n の元の間に数の演算と同じような演算が出来ることを保証している. (ただし積が可換でない, つまり $ww' = w'w$ が必ずしも成立しないので, 通常の数の演算と異なる面もある). そして, このような性質こそが置換を繰り返して新しいものを構成していくという, あみだくじのダイナミズム (それ程大層なものではありませんが) を実現しているのである. このような性質を持った演算の体系を**群**という. S_n はその一例であり n **次対称群**と呼ばれている. (以下に述べる 性質 (i) は S_n については簡単に確かめられる.) 参考のため, 以下に群の正確な定義を述べておく.

集合 G に "積 xy" $(x, y \in G)$ が与えられて次の性質をみたすとき, G を群という.

(i) (結合法則) $x, y, z \in G$ に対し, $(xy)z = x(yz)$.

(ii) どんな $x \in G$ に対しても $xe = ex = x$ となる元 $e \in G$ (単位元と呼ばれる) が存在する.

(iii) $x \in G$ に対し $xx^{-1} = x^{-1}x = e$ をみたす元 x^{-1} (x の逆元と呼ばれる) が存在する.

蛇足ながら, 群というのは英語の group の訳語である. 日本語の "群" は "群れ" という意味だが, 群れは単なる集合ではない. 「羊の群れ」とか, 「ジャッカルの群れ」 とは言うが決して「石ころの群れ」とか, 「金貨の群れ」とは言わないのである. (この場合 「金貨の山」が正しい). 群れという単語は動物に対して使われ, 動きまわるというのが絶対の前提になっているのである. その意味で, 数学的な「群」 のイメージにぴったりであり, 良くできた訳語になっている. 群論を研究している数学者は皆, 群を生き物だと思っているのです.

S_n の元 w で, 文字 i と j を入れ替えて, 他の文字は全て動かさないとき w を**互換**といい, $w = (i, j)$ と書く. また恒等置換 w_0 を (1) と書き表す. 例えば

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1,2), \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2,4).$$

Table 1 は, あみだくじの操作により

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = (3,5)(1,5)(4,5)(1,3)(1,2)$$

と w が互換の積で表されることを示している (操作の順番は右から左). 一方, あみだくじの各過程を i 番目の数字と $i+1$ 番目の数字の置換とみることにより,

$$w = (1,2)(2,3)(4,5)(3,4)(2,3)$$

と表すこともできる. この場合は操作の順番は左から右へ進む. (最初に (1,2) により 1 番目と 2 番目を入れ換え, 次に (2,3) により 2 番目と 3 番目を入れ換え ...) 互換 $(i, i+1)$ が i 番目と $i+1$ 番目の縦線を結ぶ横線に対応する. この例からも分るように, $(i, i+1)$ のような連続した数字の互換が特に

重要である. そこで次のような特別な互換の集合

$$S = \{(1,2),(2,3),\ldots,(n-1,n)\}$$

を考える. S_n の勝手な元は S の元の積で表すことができる. さらに, S_n の元 w を S の元の積で表すことと, 置換 w を与えるあみだくじを作ることが同値になる. S の各元があみだくじの横線に対応する. このようにして, あみだくじに関する問題は対称群 S_n と互換の集合 S に関する群論の問題に帰着されるのである. 次の問題を考える.

問題 1. 与えられた $w \in S_n$ に対し, 置換 w を実現するような最も効率の良いあみだくじ, つまり横線の個数を最小にするようなあみだくじを作れ.

この問題は次の群論の問題と同値になる.

問題 2. $w \in S_n$ を S の元の積として, 最小個数の S の元を使って表せ.

(もちろん, 問題 1, 2 が意味を持つためには, 最初に, どんな $w \in S_n$ も S の元の積で書けることを確かめて置かなければならない). $w \in S_n$ に対し, $w = s_{i_1}s_{i_2}\cdots s_{i_k}$ と S の元の積で表すとき, その最小個数 $k = l(w)$ を w の長さという. $l(w)$ をどのように求めるかが問題 2 の主要な部分である. 一方, $w \in S_n$ を

$$w = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ w(1) & w(2) & \ldots & w(n-1) & w(n) \end{pmatrix}$$

と表すとき

$$T(w) = \big\{(i,j) \mid 1 \le i < j \le n, w(i) > w(j)\big\}$$

とおく. $T(w)$ は w によって, 大きさの順序が逆転するような組 (i,j) の集合を表す. 例えば

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

に対しては, $T(w) = \{(1,2),(1,3),(1,4),(2,3)\}$ である. 集合 $T(w)$ の元の個数を $t(w)$ と表し, w の転倒数という. 次の定理が問題 2 に対する解答を与える.

定理 1. $w \in S_n$ に対し, $l(w) = t(w)$ が成り立つ.

実際 $t(w)$ は簡単に計算できるので, 定理 1 により $l(w)$ が容易に求まる. 講義では定理 1 の証明の概略を説明する. この問題は, 「群の生成元に関する語の問題」 と言われる群論の問題の, 特別な場合にあたる. 一般には非常に困難な問題である. 以下に n が大きい場合の例をあげておく.

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 8 & 6 & 2 & 1 & 9 & 10 & 7 & 5 & 3 \end{pmatrix}$$

を S_{10} の置換とする. この場合 $l(w) = t(w) = 23$ であり,

$$\begin{aligned} w =& (7,8)(8,9)(9,10)(6,7)(5,6)(6,7)(7,8)(8,9)(9,10)(3,4)(4,5)(5,6) \\ & (6,7)(7,8)(8,9)(9,10)(2,3)(3,4)(4,5)(1,2)(2,3)(3,4)(4,5) \end{aligned}$$

と分解できることが $t(w)$ の計算から得られる. 下図はあみだくじによる表示である. しかしこれが最小の表示であることを定理 1 を使わずに定義から直接確かめようとすれば, 22 個以下の S の元の積で書ける S_{10} の元を全部調べ, その中に w が現れないことを見ることになる. S の元は 9 個あるから, 10^{22} 回位のチェックが必要になり, 手計算では一生かかってもやりきれない. 定理 1 のありがた味がよく分かるだろう.

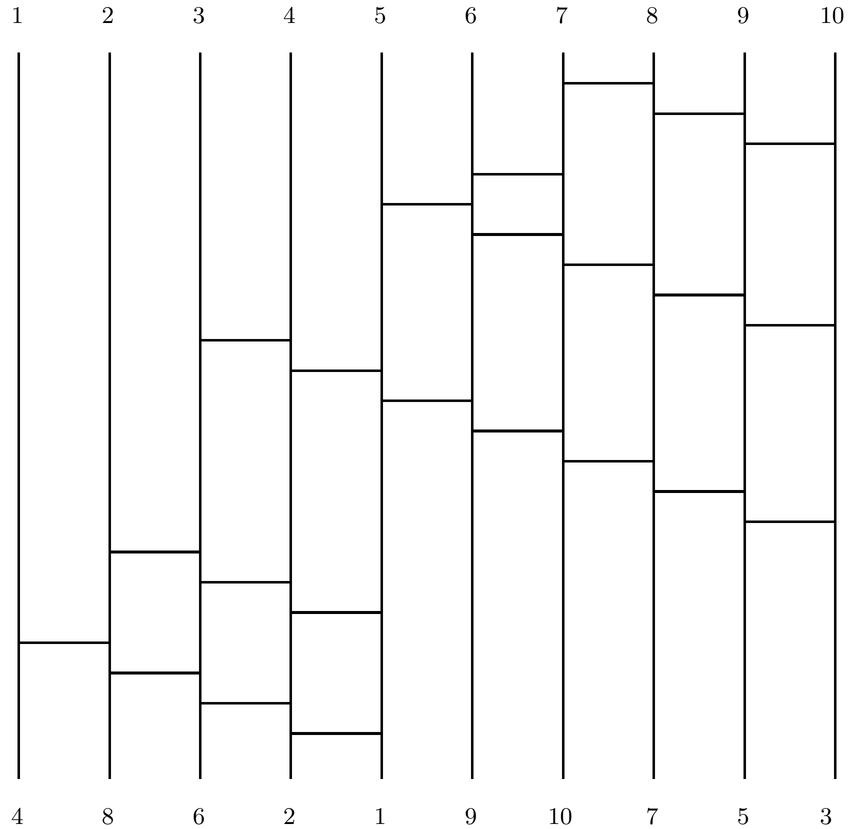


Figure 2. あみだくじの最短表示 (23 段)

あみだくじの発展問題として次を考える. あみだくじを立体化し, 何本かの柱を円周に沿って立てる. 隣り合った柱の間に横棒 (あるいはロープ) を張る. これを円筒型あみだくじ, あるいは, さる山あみだくじという. (動物園のさる山を想像して下さい). 円筒型あみだくじに対しても, 問題 1 , 問題 2 と同様の定式化ができる. この場合, 集合 S の代わりに

$$S' = \{(1,2),(2,3),\ldots,(n-1,n),(n,1)\}$$

を考えて, w を最小個数の S' の元の積として表示する公式を作ることができる. 例えば, 前の $w \in S_{10}$ については, その最小個数 17,

$$\begin{aligned} w =&(1,2)(2,3)(1,2)(3,4)(2,3)(5,6)(4,5)(3,4)(6,7)\\ &(8,9)(7,8)(6,7)(9,10)(8,9)(7,8)(1,10)(1,2)\end{aligned}$$

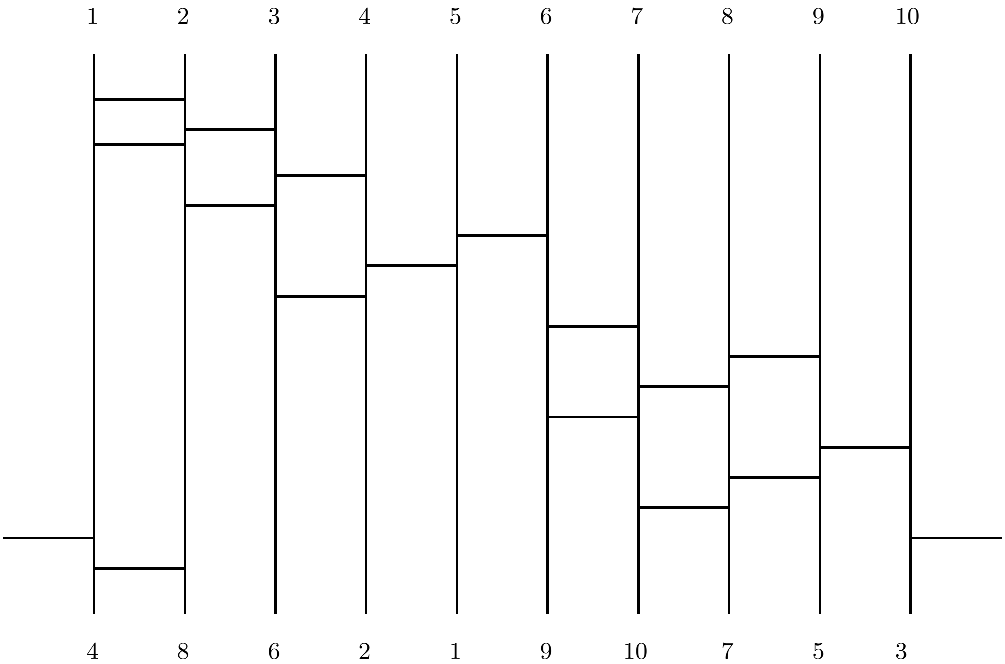


FIGURE 3. 円筒型あみだくじの最短表示 (17 段)

が w の分解を与える．上図は円筒型あみだくじによる表示を表す．両側に飛び出している線分が一番目の柱と 10 番目の柱を結ぶ横棒を意味する．

２．１５ゲーム

下図のように，１５個の数字の入った駒を空欄を使って滑らせることにより，数字をそろえて行くゲームを１５ゲームという．ここで X は空欄を表す．このゲームもまた，数字の入れ換えという置換の原理に基いて構成されている．

6	14	12	7
13	9	2	15
4	8	X	11
3	5	10	1

通常のゲームでは，１から１５の数字がそろった状態から出発し，ゲームの操作 (これを**スライド変換**と呼ぶことにする) によって，数字の順番をくずしておく．それを元に戻すのがゲームである．どのようにして戻すかが問われているわけで，戻せるということについては疑う余地はない．それではこの駒を一度全部外に出し，無秩序に入れ直した状態から出発したら元に戻るだろうか．実際にやっ

てみた人なら経験があるだろうが, うまく行かない事態も起こるのである. 何時間かのむなしい努力の後に, あきらめてしまうのであるが, それでも, もう少しやっていたら出来たかも知れないのにと未練が残ることになる.

講義では, この問題を数学的に解明する. より一般に次のような問題を考えよう. 4×4 マスの代りに, 縦 m, 横 n の $m \times n$ マスを考えて, そこに $N = nm - 1$ 個の正方形の駒を入れる. これを N ゲームということにする. あまり小さいと動きがスムースに行かないから, $m \geq 2, n \geq 4$ としておく.

問題 3. N ゲームにおいて, 駒を一度外に出して入れ直した場合, それがスライド変換により元に戻せるため必要十分条件は何か. また元に戻せない場合、どの程度元の状態に近く出来るか.

対称群 S_N を使ってこの問題へのアプローチを計る. しかし N ゲームをコントロールしているのは実は対称群ではなく, 交代群といわれる S_N の部分群 (S_N の部分集合で, S_N の演算に関して群になっているもの) である. 以下に交代群を定義しておく

１節で見たように S_n の元 w は, 互換の積として表される. 偶数個の互換の積として表されるとき w を**偶置換**, 奇数個の積で表されるとき w を**奇置換**という. これは互換の積としての表し方によらない. S の元を使っても, 一般の互換を使っても同じである. S_n の偶置換の全体を A_n とおく. 偶置換と偶置換の積はまた偶置換になることから, 偶置換の全体に積が定義され A_n は S_n の部分群になる. A_n を n **次交代群** と呼ぶ. 例えば $n = 3$ の場合,

$$(1) = (1,2)(1,2), \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2)(2,3), \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (2,3)(1,2)$$

が偶置換の全体であり, $A_3 = \{(1), (1,2)(2,3), (2,3)(1,2)\}$ が 3 次交代群 A_3 を与える. $n = 3$ の場合, 置換の全体は $3! = 6$ 個, 偶置換の全体は, 丁度半分の $3!/2 = 3$ 個ある. 一般に偶置換の個数と奇置換の個数は等しいので, A_n の元の個数は $n!/2$ である.

問題 3 は, 交代群 A_N $(N = mn - 1)$ を利用して解決することができる. 今, 縦 m, 横 n の長方形の枠の中に, $N = nm - 1$ 個の数字 $\{1, 2, \ldots, N\}$ をひとつずつ配置した図形をタブローということにする. ただし右下隅は必ず空欄 X とする. 例えば, $m = 2, n = 3$ とすると $N = 5$ であり, タブローの例として次のようなものが取れる.

$$x = \begin{array}{|c|c|c|} \hline 2 & 3 & 5 \\ \hline 1 & 4 & \mathrm{X} \\ \hline \end{array} \qquad y = \begin{array}{|c|c|c|} \hline 2 & 1 & 4 \\ \hline 3 & 5 & \mathrm{X} \\ \hline \end{array}$$

n, m を固定して, タブロー全体の集合 $\mathcal{X}$ を考える. $\mathcal{X}$ は N ゲームのゲーム状態全体の集合と思ってもよい. $x, y \in \mathcal{X}$ に対し, y が x からスライド変換によって得られるとき $x \sim y$ と表す. スライド変換の逆変換もスライド変換なので, $x \sim y$ ならば $y \sim x$ である.

さらに $x \in \mathcal{X}$ に対して, x 内の数字 $1 \sim N$ を左から右へ, 上から下へ並べてできる列 ($1 \sim N$ の順列) を $[x]$ と表す. x, y が上の例の場合, $[x] = (2,3,5,1,4), [y] = (2,1,4,3,5)$ となる.

また $x, y \in \mathcal{X}$ に対し, $w[x] = [y]$ となる $w \in S_N$ が唯ひとつ定まる. 上の例の場合

$$w = \begin{pmatrix} 2 & 3 & 5 & 1 & 4 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

である. タブロー x_0, x_1 を次のように定める.

$x_0 =$

1	2	$\cdots$	n-2	n-1	n
n+1	n+2	$\cdots$	2n-2	2n-1	2n
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	N-1	N	X

$x_1 =$

1	2	$\cdots$	n-2	n-1	n
n+1	n+2	$\cdots$	2n-2	2n-1	2n
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	N	N-1	X

x_0 は数字の順番がすべてそろっている元の状態, x_1 は x_0 から $N-1$ と N をひっくり返してできるタブローである. 次の定理が問題 3 に対する解答を与える.

定理 2. $n \geq 4, m \geq 2$ (または, $n \geq 2, m \geq 4$) とし, $N = nm - 1$ とおく.

(i) $x, y \in \mathcal{X}$ に対し, $x \sim y$ となる必要十分条件は $w[x] = [y]$ で定まる w が交代群 A_n に含まれることである.

(ii) $x \in \mathcal{X}$ に対し, $[x] = (a_1, a_2, \ldots, a_N)$ とおく. $w = \begin{pmatrix} 1 & 2 & \cdots & N \\ a_1 & a_2 & \cdots & a_N \end{pmatrix}$ が偶置換ならば, $x \sim x_0$, 奇置換ならば $x \sim x_1$ となる. (しかも x_0 と x_1 はスライド変換では移りあえない).

3. ルービック・キューブ

ルービック・キューブ は多くの人が一度は手に取った経験があるのではないだろうか. 私が買ったルービック・キューブのカバーに 20 世紀最高のパズルと書いてあったが, あながち誇張とは言えない. 単純ですっきりした外観の蔭に, 非常に複雑なパターンを秘めており, 有数の数学的パズル（ゲーム？）であることは間違いない.

ルービック・キューブは, 数学的にも, あみだくじや 15 ゲームとは比べものにならない程の複雑で興味深い構造を持っている. 講義では, 前例にならってルービック・キューブの動きをコントロールしている群を決定する. 巷では, この群をルービック・キューブ群と呼んでいるようである. 以下では略してルービック群ということにする.

ルービック・キューブはひとつひとつの小さい立方体（サイコロと呼ぶ) に分解できる. 図の A のように, 各面の中心にあるサイコロは取り外せない. B の位置にあるサイコロを辺のサイコロ, C の位置にあるものを頂点のサイコロという. ルービック・キューブの動きを繰り返すことによって得られる変換を**ルービック変換** と呼ぶ. ルービック変換により, 頂点, 辺, 中心の位置にあるサイコロはそれぞれ, 頂点, 辺, 中心に移る. そこで中心にある 6 色のサイコロを固定することによって, キューブ全体の位置を定める. 以後ルービック変換により中心のサイコロは動かないとしてよい. (実際は回

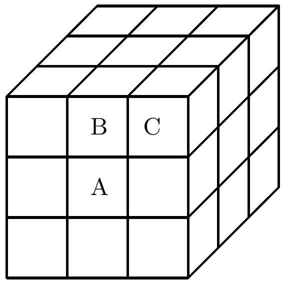


Figure 4. ルービック・キューブ $(3\times 3\times 3)$

転もあり得るが, それは区別しない). このような設定でルービック変換全体で作られる群がルービック群に他ならない.

ルービック・キューブの場合も 15 ゲームと同様に, 各面の色が全てそろった初期状態から出発し, ルービック変換によりごちゃまぜ状態を作る. そこから元の状態に戻すのがゲームである. そこで前と同様に次の問題を考える.

問題 4. ルービック・キューブを分解し, 頂点と辺にあるサイコロを全て取り外した後, 適当にはめこんでルービック・キューブを作る. それが ルービック変換によって元に戻るための条件は何か. また、このようにして得られるパターンで, ルービック変換によって互いに移り合えないものは, いくつあるか.

問題 4 を解く鍵がルービック群の決定である. 実はルービック・キューブの解法も, ルービック群を決定する過程に基本的に含まれている. ルービック群の決定は, 頂点に関するルービック群と, 辺に関するルービック群に分けて行う. 頂点に関するルービック群は, 辺を無視して 8 個の頂点サイコロの動きのみに注目して得られる群であって, $2\times 2\times 2$ の場合のルービック群と同じものである.

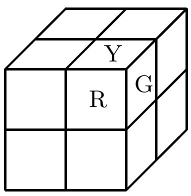
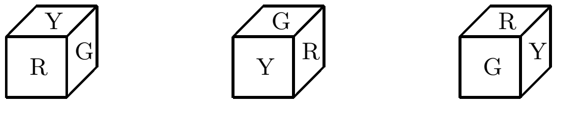


Figure 5. $2\times 2\times 2$ 型ルービック・キューブ

講義では主にこの場合を扱う. バラした頂点サイコロを戻すには 8 個の位置が選べる. さらに一つの位置を決めた場合でも, 頂点サイコロは次のような 3 種類のはめ込み方ができる.



これらは, 立方体の頂点と中心を結ぶ軸のまわりの 120 度の回転に対応している. そこで, ここでは 8 個の頂点の置換から得られる対称群 S_8 と各頂点での 120 度回転を混ぜあわせた群が主役を演じる

ことになる．それは**回転付き置換** からできる群で複素鏡映群と呼ばれる群の一種である．そのような群を記述するために少し準備がいる．

まず, 回転の群から始める．r を正の整数として $\theta = 360°/r$ とおく．α を角度 θ の回転とすると, $\alpha^r = 1$ (ゼロ回転) である．

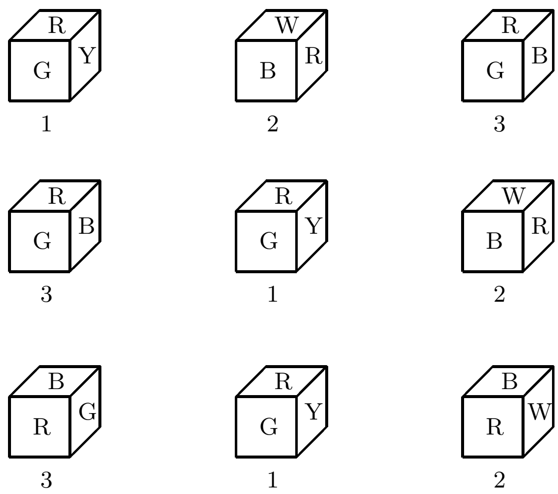
$$C_r = \{\alpha^0 = 1, \alpha, \alpha^2, \dots, \alpha^{r-1}\}$$

は回転の合成, $\alpha^i \alpha^j = \alpha^{i+j}$ により群になる．(単位元は $\alpha^0 = 1$, α^i の逆元は α^i の逆回転 $\alpha^{-i} = \alpha^{r-i}$). C_r を r **次巡回群**という．例えば $r = 3$ の場合, α は 120 度の回転であり, $C_3 = \{\alpha^0, \alpha^1, \alpha^2 = \alpha^{-1}\}$ である．

次に回転付き置換を導入する．次の例を考えよう．(R, Y, G), (W, R, B), (R, B, G) の 3 色からなる頂点サイコロ 3 個に, 1, 2, 3 と番号をつけておく．まず $w \in S_3$ によって, サイコロを置換し, 次いで各サイコロをその場で回転させる．

$$w = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ \alpha^0 & \alpha^2 & \alpha^1 \end{pmatrix}$$



この操作を回転付き置換といい,

$$A \cdot w = \begin{pmatrix} 1 & 2 & 3 \\ \alpha^1 \cdot 3 & \alpha^0 \cdot 1 & \alpha^2 \cdot 2 \end{pmatrix}$$

と表す．一般に n 次対称群 S_n と r 次巡回群 C_r が与えられたとき, $w \in S_n$ と $A \in (C_r)^n$ (n 個の C_r の組) に対して, 回転付き置換 $A \cdot w$ が定義される．回転付き置換の集合

$$G = \{A \cdot w \mid w \in S_n, A \in (C_r)^n\} = S_n \cdot (C_r)^n$$

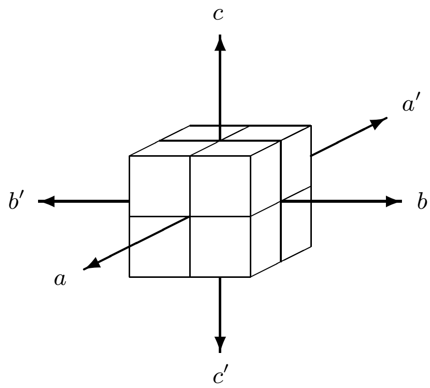
は群になる．これを $G = G(r, 1, n)$ と表す (G と C_r のレス積ともいう)．G の元は S_n の元と $(C_r)^n$ の元の積として一意的に表されるので, G に含まれる元の個数は $n! \times r^n$ である．頂点に関するルービック群の場合, 頂点サイコロが 8 個, 各頂点での回転が 120 度なので, $n = 8, r = 3$ の場合, すなわち群 $G = G(3, 1, 8)$ が怪しい群として候補にあがる．しかし N ゲームの場合にゲームを支配する群

は交代群 A_N であって, 対称群 S_N ではなかったように, 今の場合も $G(r,1,n)$ よりも少し小さい群を考える必要がある. そこで, $A\cdot w \in G(r,1,n)$, $A=(\alpha^{i_1},\dots,\alpha^{i_n})\in (C_r)^n$ に関して次の条件を考える.

$$(*) \qquad \alpha^{i_1}\alpha^{i_2}\cdots\alpha^{i_n}=1 \iff i_1+i_2+\cdots i_n \text{ は } r \text{ の倍数}.$$

$G_0=\{A\cdot w\in G(r,1,n) \mid A \text{ は } (*) \text{ を満たす}\}$ とおく. G_0 は G の部分群になる. $G_0=G(r,r,n)$ と表す. G_0 の元の個数は $n!\times r^{n-1}$ である. 頂点に関するルービック群の場合 $n=8, r=3$ であるから $G_0=G(3,3,8)$ が問題になる. この場合 G_0 の元の個数は $8!\times 3^7$ で与えられる.

$2\times2\times2$ 型ルービック・キューブの場合, ルービック変換は軸 a, 軸 a' を中心とする 90 度回転, 軸 b, 軸 b' を中心とする 90 度回転, 軸 c, 軸 c' を中心とする 90 度回転, の 6 種類の操作を組み合わせて得られる.

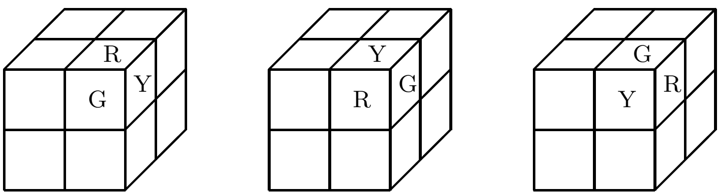


これらの 6 種類の操作により, 頂点サイコロの回転付き置換が引き起こされる. そこで頂点に関するルービック群 H_V ($2\times2\times2$ 型ルービック・キューブ群) は $G(3,1,8)$ の部分群とみなすことができる. 講義では次の定理を示す.

定理 3. $2\times2\times2$ 型ルービック・キューブに関して次が成り立つ.

(i) $H_V=G(3,3,8)$.

(ii) キューブをばらして組み立て直したものは, ルービック変換により次のいずれかに移る.



元の状態　　120 度回転　　240 度回転

(1 番目のキューブは前面 G (緑), 上面 R (赤), 右面 Y(黄色) と 6 面の色がそろった元の状態のキューブである. 2 番目はそれから, (R,G,Y) のコーナーのサイコロのみを 120 度回転させてできたもの (他の部分は全て 1 番目と同じ), 3 番目は 240 度回転させてできたキューブを表す. この 3 つはルービック変換では互いに移りあえない.)

今まで頂点に関するルービック・キューブ群について調べて来たが, 同様の議論が辺に関するルービック群についても成立する. 辺サイコロは 12 個あり, それぞれに関して 180 度の回転が考えられる. そこで辺の場合には $G(2,1,12) = S_{12}.(C_2)^{12}$ とその部分群 $G(2,2,12)$ を考えることになる. 実際, 辺に関するルービック・キューブ群 H_E は $G(2,2,12)$ に一致し, バラして組み直した場合表れるパターンは 2 種類 (元の状態, 一つの辺サイコロを 180 度回転させたもの) になることが確かめられる.

本来のルービック群 H は H_V と H_E を組み合わせて記述することができる. この辺の議論にはより進んだ群論の知識が必要になるが結果のみを記すと次のようになる. $H_V \times H_E$ を $g \in H_V$ と $h \in H_E$ の組 (g,h) の全体とする. $H_V \times H_E$ には自然に群の構造が入る. これを H_V と H_E の直積の群という. H は $H_V \times H_E$ の部分群になり, その元の個数は $H_V \times H_E$ の元の個数の半分である. 特に $|H|$ を H の元の個数とすると

$$|H| = \frac{1}{2}(8! \times 12! \times 3^7 \times 2^{11}) = 43252003274489856000$$

で与えられる. より精密には次のようになる. $S_8 \times S_{12}$ を対称群 S_{21} の部分群とみる (S_8 は文字 $\{1,2,\ldots,8\}$ の置換, S_{12} は $\{9,10,\ldots,21\}$ の置換と考える). $A(S_8 \times S_{12})$ を $S_8 \times S_{12}$ の中で, S_{21} の偶置換からなるものの全体とする. $A(S_8 \times S_{12})$ は $S_8 \times S_{12}$ の部分群で, その元の個数は丁度半分になる. $H_V \simeq S_8 \cdot (C_3)^7$, $H_E \simeq S_{12} \cdot (C_2)^{11}$ と表すとき

$$H \simeq A(S_8 \times S_{12}) \cdot ((C_3)^7 \times (C_2)^{11}).$$

ルービック・キューブをバラして組み直すとき, 頂点サイコロの回転付き置換で, $8! \times 3^8$ 個のパターンが生じる. 辺サイコロの回転付き置換からは, $12! \times 2^{11}$ 個のパターンが生じる. 従って組み直した時に生じるパターンの総数は

$$(8! \times 3^8) \times (12! \times 2^{12})$$

である. 一方, 元の状態からルービック変換により得られるパターンの総数は H の元の個数で与えらる. 両者を比較することにより, バラして組み直したときルービック変換で移り合えるのは $2 \times 3 \times 2 = 24$ 種類のパターンに分かれることが導かれる. また, 組み直したキューブがルービック変換で元に戻せるかどうかは, N ゲームの場合と同様に, 組み直したものを元の状態と比較して, 頂点と辺に関する回転付き置換として表し, それが H の含まれるかどうかによって判定される. これが問題 4 の答である.