イプシロン　2013.Vol.55, 87 – 92

群論マジック

愛知教育大学初等教育教員養成課程数学選修3年　伊　東　桂　司

概 要

毎年夏に開かれるオープンキャンパスにて「模擬授業」と称して数学マジックを生徒さんたちに見てもらっています．その一つのネタに手品師ボブ・ハマーが考案したといわれる「３つの品の手品」というのがあります（本論ではカードで説明していますが，普段は３匹のぬいぐるみで行っています）．これは演じやすく，また観客にもルールは分かり易いのですが，なぜ観客が選んだ品を演者がすぐに当てられるのか，なかなか見破られないという数理論理の優れたネタです．ある日，伊東君に「このネタは長年やっているのだけど，これを４つ以上の品の手品にできないだろうか？」と何気なく問題提起したところ，クラインの四元群を利用したうまい手品を彼が思いつきました．それまで私は「背理法のパズル」のつもりでやっていたわけですが，彼はこれを置換の話題だと見抜き，その場で新しい手品を作り上げたのです！　　（数学教育講座 橋本行洋）

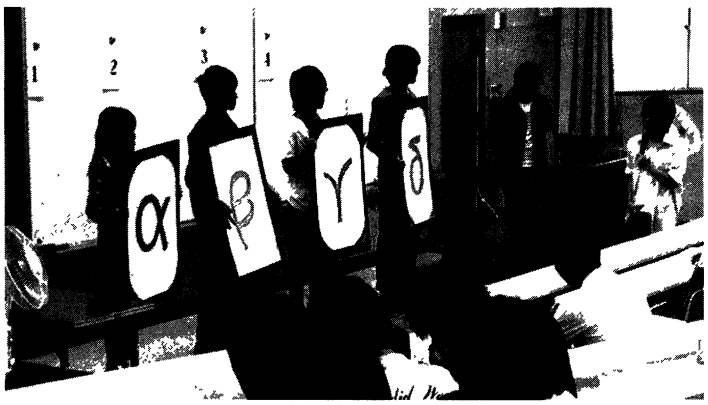

図 1: オープンキャンパス 2013/07/28 より

1　はじめに

３枚のカードを用意する．ゲストは１枚のカードを選び，指定されたカードの入れ替えを行う．マジシャンは，その選ばれたカードを当てることが目的である．

2　３枚の場合

まずは，ルールを説明する．

1. カードを３枚用意して並べる．マジシャンは，その配置を確認する．

2. ゲストは，カードを１枚選ぶ．

3. ゲストは，(1 2), (1 3), (2 3) の入れ替えを何度か行う．このとき，どの入れ替えを行ったのかのみを，マジシャンに知らせる．

4. ゲストは，一度だけ"秘密"という操作を行う．
"秘密"という操作は，選んだ１枚のカード以外の残りの２枚を移動させる操作である．
マジシャンには,「秘密」と伝える．

5. ゲストは再び，(1 2), (1 3), (2 3) の入れ替えを何度か行う．このときも同様に，どの入れ替えを行ったかをマジシャンに知らせる．

6. マジシャンは，最後の配置を見て選んだカードを当てる．

※ $(a\ b)$ は，置換の記号と考え，a と b を入れ替えるという意味を表す．

以上のルールで，マジシャンはカードを当てる．どのように当てればよいのだろうか．３枚のカードすべての入れ替えを頭の中で追うことは難しい．また,「秘密」による移動で，どの２枚を入れ替えるのか分からない以上，ゲストが選んだカードを当てるのは難しい．

では，どのようにすればよいのだろうか．マジシャンはカードを１枚選び，それを追えばよいのである．「秘密」の入れ替え以外は，１枚のカードであれば，頭の中で追うことは易しい．焦点となるのは,「秘密」の操作である．ゲストの選んだカードとマジシャンの選んだカードが一致していれば，そのカードは「秘密」によって移動しない．したがって,「秘密」の操作では，マジシャンは何も移動していないと考えればよいのである．そうすれば，マジシャンが最後の配置を確認したときに，自分の選んだカードは正しい位置にある．よって，そのカードがゲストの選んだカードである．それでは，ゲストのえらんだカードとマジシャンの選んだカードが異なる場合はどうなるだろうか．こちらも同様に,「秘密」の操作は，何も移動しないと考える．すると，マジシャンが最後の配置を確認したときに，自分の選んだカードがあるはずの場所に，他のカードがあるはずである．つまり,「秘密」の操作によって，自分の選んだカードと，自分の選んだカードがあるはずの場所にあるカードの２枚が入れ替わったわけである．したがって，ゲストが選んだカードは残りの１枚である．

では，カードを４枚に増やすとどうなるだろうか．

3　４枚の場合

基本的なルールは３枚のときと変更はない．注意すべき点は，カードの入れ替え方が異なる点である．４枚の場合では，次の A, B, C の３種類の入れ替え方を行う．

$$A:\ (1\ 2)(3\ 4),\ B:\ (1\ 4)(2\ 3),\ C:\ (1\ 3)(2\ 4)$$

また,「秘密」の操作にも気をつける．秘密では，最初に選んだカード以外の残り３枚をすべて移動させる．そうすることによって，４枚の場合でも，ゲストが最初に選んだカードを当てることができる．

どのようにしてカードを当てるのか説明する．以下，カードの入れ替えは，先に実行するものを右に書くことにし，演算として$\cdot$の記号を用いることとする．例えば，Aの操作のあとにBの操作を行った場合$B\cdot A$と書くことにする．この記号を用いると，

$$\begin{aligned} A\cdot B &= B\cdot A = C,\\ B\cdot C &= C\cdot B = A,\\ C\cdot A &= A\cdot C = B \end{aligned}$$

が成り立つ．また，何も動かさないことをe（単位元と考える）と表すことにすると，明らかに

$$A\cdot A = B\cdot B = C\cdot C = e$$

が成り立つ．つまり，A,B,Cの入れ替えを何回か行っても，e,A,B,Cの４つの入れ替えのうちのどれかを１回行ったことと変わらないのである．

「秘密」の操作によって，ゲストが選んだカード以外の残りの３枚はすべて移動していることを考慮すると，マジシャンは，秘密の操作を除いたA,B,Cの操作を順番に追うことで，最後にe,A,B,Cのどれかになっていると判断することができ，正しい位置にあるカードが，ゲストの選んだカードであると分かる．

では，実際にマジックを行うと，どのようになるのか確認してみる．４つの文字$\alpha,\beta,\gamma,\delta$が書かれたカードを用意して

$$\alpha\ \beta\ \gamma\ \delta$$

の順で並べたとする．ここで，マジシャンはこの配置を確認する．ゲストははじめにカードを１枚選ぶので，ここではαを選んだとしよう．そして，ゲストがA,B,Cの移動の仕方を選び，カードを移動させる．以下，実際に操作を行ってみる．

$$\alpha\ \beta\ \gamma\ \delta \xrightarrow{A} \beta\ \alpha\ \delta\ \gamma \xrightarrow{B} \delta\ \gamma\ \beta\ \alpha \xrightarrow{A} \gamma\ \delta\ \alpha\ \beta \xrightarrow{\text{秘密}} \beta\ \gamma\ \alpha\ \delta \xrightarrow{C} \delta\ \alpha\ \gamma\ \beta \xrightarrow{B} \gamma\ \beta\ \delta\ \alpha$$

毎回，カードの配置を書いたが，マジシャンには，A,B,Cと”秘密”のみしか伝わっていない．そこで，マジシャンはA,B,C着目して，最後の配置は，どの操作で表されているのかを考える．実際に計算すると

$$B\cdot C\cdot A\cdot B\cdot A(\alpha\ \beta\ \gamma\ \delta) = C(\alpha\ \beta\ \gamma\ \delta)$$

であるので，最後の配置は，最初の配置からCの操作を行っただけであるとわかる．$C\cdot C = e$であることを考えると，最後の配置にもう一度Cを行うと，もとに戻るはずである．実際に行ってみると

$$\gamma\ \beta\ \delta\ \alpha \xrightarrow{C} \alpha\ \delta\ \beta\ \gamma$$

となり，きちんともとに戻るのはαだけである．これは，”秘密”によって他の３つが移動したことにより，もとの位置に戻らなくなるためである．したがって，ゲストが選んだカードはαである．

4 $2n$ 枚の場合

更にこれを一般化することはできないだろうか．カードが４枚のときは，対称群 S_4 の部分群となるような置換を用意して，それをカードの入れ替え方とした．それにしたがって，今回のマジックに適するような S_m の部分群を探したい．そのために以下の３つを仮定した．

【1】部分群 H に元 $\sigma,\tau(\sigma \neq \tau)$ が存在して，$<\sigma,\tau>= H$ (H は σ,τ の２元で生成される) であること．

【2】１の σ,τ に対し，$\sigma^2 = \tau^2 = e$ であること．

【3】部分群 H の単位元 e を除く任意の元 g が，$i(= 1,2,\cdots,m)$ に対し，$g(i) \neq i$ であること．

まずは，生成元について考える．

定理 4.1 生成元 σ は，互換の積で表される．さらに，各 $i(i = 1,\ldots,m)$ は１度しか現れない形で σ を表現することができる．

(証明) $i(i = 1,\ldots,m)$ は σ によって $j(j = 1,\ldots,m, i \neq j)$ に移されるとする．$\sigma(j) \neq i$ であると，$\sigma^2(i) = i$ であることに矛盾する．したがって σ は互換 $(i\ j)$ を互換にもつ．また，仮定【3】より，すべての i がどれかの互換によって移されなければならない．したがって，m が奇数の場合は，考えることができない．$m = 2n$ のとき，S_{2n} は互換の積で表される．

次に，σ が互換 $(i\ j),(i\ k)$ $(k = 1,\ldots,m)$ の２つをもったとする．これらの互換の積は巡回置換 $(i\ j\ k)$ となる．これは，位数が３であり仮定【2】に反する．これは i が３回以上現れた場合も同様である．したがって，i が１度しか現れない形で σ を表すことができる． □

また，τ も同様に，互換の積で表される．

定理 4.2 $H =<\sigma,\tau>$ とすると，σ と τ は共通の互換をもたない．

(証明) $\sigma,\tau(\sigma \neq \tau)$ は共通の互換をもつと仮定すると，$\sigma(i) = \tau(i) = j, \sigma(j) = \tau(j) = i$ となる $i,j(i,j = 1,\ldots,n$ かつ $i \neq j)$ が存在する．すると，$\tau\cdot\sigma(i) = i$ となり，仮定【3】に反する．したがって，σ と τ は共通の互換をもたない． □

この定理により，σ,τ を具体的に定めるアルゴリズムが作られる．ある a_1 に対し $a_2(\neq a_1)$ が存在して，$\sigma(a_1) = a_2$ とする．次に，その a_2 に対し a_3 が存在して，$\tau(a_2) = a_3$ とする．このとき，定理4.2より，$a_3 \neq a_1$，仮定【3】より，$a_3 \neq a_2$ である．次に，$\sigma(a_3) = a_4$ とすると，a_1, a_2, a_3 はすでに σ の置換に現れているので $a_4 \neq a_1, a_2, a_3$ である．同様に，$\tau(a_4) = a_5$ とすると，$a_5 \neq a_2, a_3, a_4$ である．しかし，$2n > 4$ のとき，$\tau(a_4) = a_1$ の場合と $\tau(a_4) \neq a_1$ の場合に場合分けする必要がある．ちなみに，$2n = 4$ の場合は，$\tau(a_4) = a_1$ となるしかないため，問題はおきない．

まずは，$\tau(a_i) \neq a_1(i = 2,4,6,\ldots,2n-2)$ となる場合を調べる．このとき，

$$a_1, a_2, \cdots, a_{2n-1}, a_{2n}$$

という数列ができる．$\tau(a_{2n}) = a_1$ とすれば，

$$\sigma = (a_1\ a_2)(a_3\ a_4)\cdots(a_{2n-1}\ a_{2n}),$$
$$\tau = (a_2\ a_3)(a_4\ a_5)\cdots(a_{2n}\ a_1)$$

と表される．そこで $\tau\cdot\sigma$ の位数を考えると，

$$\tau\cdot\sigma = (a_1\ a_3\ \cdots\ a_{2n-1})(a_{2n}\ a_{2n-2}\ \cdots\ a_2)$$

つまり，長さ n の巡回置換を2つ並べたものになるので

$$(\tau\cdot\sigma)^n = e$$

となる．したがって，$\tau\cdot\sigma$ の位数は n である．

次に，ある $i(=2,4,6,\ldots,2n-2)$ に対し，$\tau(a_i) = a_1$ となる場合を調べる．このとき，

$$\sigma = (a_1\ a_2)(a_3\ a_4)\cdots(a_{i-1}\ a_i)(a_{i+1}\ a_{i+2})\cdots,$$
$$\tau = (a_2\ a_3)(a_4\ a_5)\cdots(a_i\ a_1)(a_{i+2}\ a_{i+3})\cdots$$

となる．$i = 2k$ とおけば，さきほどと同様にして

$$(\tau\cdot\sigma)^k = e\cdot(a_{i+1},\ldots,a_{2n}\text{の置換})$$

という形になってしまい，$a_1, a_2, \ldots, a_i$ は動かない．これは仮定【3】に反する．

以上の議論により，部分群 H を特徴付けるために新しい仮定を追加する．

【4】$\tau\cdot\sigma$ の位数は n である．

さて，H の元がどのような形なのかについて，少しみていきたい．

定理 4.3 H の任意の元は $\cdots\tau\cdot\sigma\cdot\tau\cdot\sigma$ という σ,τ を交互に並べた形で表される．

(証明) H の任意の元 g を

$$g = \cdots\tau^{j_4}\cdot\sigma^{j_3}\cdot\tau^{j_2}\cdot\tau^{j_1}$$

と，σ と τ のべき乗の積の形で表せたとする．$\sigma^2 = \tau^2 = e$ より，$j_s(s = 1,2,\cdots)$ は0か1で十分である．$\sigma^0 = \tau^0 = e$ であるので，g は

$$g = \cdots e\cdot\sigma\cdot\tau\cdot\tau$$

のような形に書き直すことができる．そこで，g を右から順に見ていく．$\cdots\sigma\cdot\sigma\cdots$ か $\cdots\tau\cdot\tau\cdots$ のように，同じ置換が2つ続いていたらその部分は e となる．この操作を，これ以上できなくなるまで繰り返す．すると，g は

$$g = \cdots\sigma\cdot\tau\cdot\sigma$$

もしくは，

$$g = \cdots\tau\cdot\sigma\cdot\tau$$

という形のどちらかになる．$g = \cdots\sigma\cdot\tau\cdot\sigma$ の場合は，求めるものになる．

以下，$g=\cdots\tau\cdot\sigma\cdot\tau$ の場合について考える．

$$g=\underbrace{\cdots\tau\cdot\sigma\cdot\tau}_{\text{長さ } p}$$

とする．p を $2n$ で割ったときの商を q とすると，$(\tau\cdot\sigma)^n=e$ であることより

$$\begin{aligned}g&=\cdots\tau\cdot\sigma\cdot\tau\\&=\cdots\tau\cdot\sigma\cdot\tau\cdot(\tau\cdot\sigma)^{n(q+1)}\\&=\cdots\sigma\cdot\tau\cdot\sigma\end{aligned}$$

となり，求めるものになる． □

また，これより次のことが分かる．

定理 4.4 H の位数は $2n$ である．

（証明） $g_1,g_2\in H$ で，

$$g_1=\underbrace{\cdots\sigma\cdot\tau\cdot\sigma}_{\text{長さ } i_1},\quad g_2=\underbrace{\cdots\sigma\cdot\tau\cdot\sigma}_{\text{長さ } i_2}$$

と表せる $(i_1,i_2=0,1,\ldots,2n-1)$．ここで，$i_1\neq i_2$ のとき，$g_1=g_2$ と仮定すると

$$\underbrace{\cdots\sigma\cdot\tau\cdot\sigma}_{\text{長さ } i_1}=\underbrace{\cdots\sigma\cdot\tau\cdot\sigma}_{\text{長さ } i_2}$$

すなわち，

$$\underbrace{\cdots\sigma\cdot\tau\cdot\sigma\cdots}_{\text{長さ } i_1-i_2}=e$$

となり，仮定【4】に矛盾する．したがって，$i_1\neq i_2$ のとき，$g_1\neq g_2$ である．よって，H の位数は $2n$ である． □

以上のことにより，今回のマジックはカードが $2n$ 枚であれば，S_{2n} の部分群で位数が $2n$ のものを作ることができる．たとえば，$2n=6$ であれば，1つの例として

$$\sigma=(1\ 2)(3\ 4)(5\ 6),\quad \tau=(2\ 3)(4\ 5)(1\ 6)$$

を考えることができる．これらから生成される部分群は次の6つの元

$$\begin{gathered}e,\quad \sigma=(1\ 2)(3\ 4)(5\ 6),\quad \tau\sigma=(1\ 3\ 5)(6\ 4\ 2),\\ \sigma\tau\sigma=(1\ 4)(2\ 5)(3\ 6),\quad \tau\sigma\tau\sigma=(5\ 3\ 1)(2\ 4\ 6),\\ \tau=\sigma\tau\sigma\tau\sigma=(2\ 3)(4\ 5)(1\ 6)\end{gathered}$$

からなる．この部分群を用いれば，σ,τ の個数を数えて，6で割った余りを考えることによって，マジックを行うことができる．