

# 数学の危機なのか、 数学教育の危機なのか —(美杉セミナー'94)—

蟹江 幸博  
三重大学教育学部

## 目次

1	はじめに	1
2	TOSM ポストのその後	2
2.1	TOSM ポストの質問集	2
2.2	ハノイの塔の柱が4本になったらどうなるのか？	5
2.2.1	ハノイの塔とは	5
2.2.2	ハノイの塔の状態の表し方	5
2.2.3	ハノイの塔の最短手順	7
2.2.4	具体的な手順の例	12
2.3	空集合の記号の読み方	17
2.4	対偶による証明法と背理法との違い	18
2.5	論理(数学のグラマー)[「小学校教師の数学的常識」より]	21
3	アミダくじと組み紐の群(美杉セミナー'94)	27
3.1	対称群とアミダ群	27
3.2	アミダ群の特別な元	35
4	終わりに	40

## 1 はじめに

1994年度は日本数学教育学会の全国大会の準備・運営など大変ご苦労様でした。何のお手伝いも出来ず、心苦しく思っておりました。大会のため、近年恒例となっている美杉セミナーを夏休みに開くことが出来ず、冬休みにという話しも立ち消えになり、色々な

経緯はありましたが、結局「高校生セミナー」という名で、3月11日に四日市駅前のじばさん三重、12日には四日市高校で行われました。

主催された桑名高校の中条政紀先生は、1日目は数学だけでなく、理科系全般にわたる講演の形で行いたいというご意向でした。三重大学の中で講師はいないかというご依頼で、硬い理科系の代表として素粒子論の阿閉義一・教育学部教授と、柔らかい分野の代表として森林育成学の永田洋・生物資源学部教授を推薦したところ、両氏とも快く引き受けて下さり、熱意溢れる講演がありました。筆者も一講座を受け持ちました。第3節はその講演の記録です。

来年度からこの催しをどのようにして行くのかという問題は、三重県高数研としてはある意味ではっきりした態度を示しておかねばならない問題ではないかと思われます。昨年度より、文部省の大臣官房の管轄で、高校生にたいする教育上の例外措置というパイロット事業が行われています。具体的に行われた内容は、10程度の大学と団体の行う数学と物理に関する高校生に対する公開講座のようなものですが、名古屋大学などではそこでの修了を当該大学の当該学科に入学した場合に限ってはいますが、大学における単位に認定しているという動きがあります。

4月には突然の新聞報道があり、この件が拡大されて報じられたようですが、これが単なるアドバルーンなのかどうかには関心を持ちつづける必要がありそうです。

三重県の場合、数年前から高数研の先生方の熱意と三重大学教官の協力により、単位の問題は別として、実質的に行われていることであるという認識は内外共に持っているのではないのでしょうか。この種のことは、文部省主導でなされるのか、教員の熱意の顕れとしてなされるのかでは大きな隔たりがあると思います。

それゆえ、この件に関して、高数研としてきちんとした姿勢をお持ちになることが肝要かと思っております<sup>1</sup>。

ところで、高校生ばかりでなく、初等教育・高等教育における数学離れの風潮は顕著です。日本数学会でもこれまで座視していたことを反省し、理事会において「大学における数学基礎教育」や「数学の将来」の問題に関して検討するワーキンググループが作り、活動を始めております。遅きに失したというお叱りはあるかと思ひますし、また何が出来るのかという疑念もおありのことと思ひますが、暖かく見守りまた協力して頂けると有り難いと思っております。

また、数学会の体質も改善し、少なくとも高校の数学の先生方に喜んで入会して頂けるような学会に変えて行くべきだという意見も強くなつて来ております。現実的には過去のしがらみもあり簡単ではないと思ひますが、数学会への提案がございましたらいつでも取り次ぎ、実現に努力して行きたいと考えております。

また、上述の数学会のワーキンググループでもインターネットを利用し、www サイトやftp サイトを作つて情報の公開・交換を行うことを始めております<sup>2</sup>。高等学校でも、学校

<sup>1</sup> 高校生に対する数学講座の名称を、この辺りで統一して一貫性を主張した方が良いのではないのでしょうか。「第何回三重高校生数学セミナー」とするか、美杉村で始めたことを記念して場所は変わったとしても「第何回美杉セミナー - 高校生・数学の集い」とするのは如何でしょうか。この文章では一貫性を重視して、「美杉セミナー'94」という名称で呼ばせてもらうことにしました。

<sup>2</sup> モザイクや Netscape を使える環境があれば、京都大学理学部数学教室にワーキンググループの www サイトがありますので、アクセスしてみてください。

単位や学科単位でインターネットに入られているところ、また入ることを考慮されているところがあると聞いておりますが、例えば TOSM ポストのような質問箱を、高数研の執行部かどこかの高校の数学か、また総合教育センターのようなところの [www](#) サイト、または（管理の仕方が問題かもしれませんが）BBS のようなものとして開設することも考えていく必要があるかもしれません。

## 2 TOSM ポストのその後

TOSM グループの活動は細々乍ら続けておりますが、この時点でご紹介出来るようなものはポストくらいのものであります。去年からの分はやっと第 4 回 TOSM ポストとして以下にあげる 3 つの質問があるだけです。時間は掛かっても必ず、何等かの回答をさせていただきますので、これからも奮って算数・数学教育上の疑問点を、三重大学教育学部数学教室内 TOSM 三重ポストまでお送り下さい。勿論、TOSM 福井ポスト・岐阜ポストに投函されても同様にグループとして責任をもって回答させていただきます。

### 2.1 TOSM ポストの質問集

どんな質問を受け付けていることかを示すために、ここまでに投函された質問のリストを挙げておきます。

#### 1. 第 1 回 TOSM ポストの質問

- (a) 辺の長さがすべて異なる直方体の展開図はどれだけあるか？
- (b) 円周上に  $n$  点を取り互いに線分で結ぶとき、円内にできる領域は最大幾つか？ $n$  だけで簡単に表わされるか？
- (c) 正多角形を描きたい。円を使って描くように指導してある教科書があるが  $360^\circ$  を辺の数で割って整数にならないもの、例えば正 7 角形や正 11 角形などを分度器とコンパスで描くことが出来るか？
- (d) 直三角柱がある。すべての側面を横断するように平面で切った切り口は三角形になるが、正三角形になることがあるか。あるとしたらその長さは底面の三角形だけで一意的に定まっているか。出来れば底面を与えたとき、その正三角形を簡単に描くことが出来るか？
- (e)  $\sqrt{24x^2 + 8x + 1}$  が有理数となる有理数  $x$  にはどんなものがあるか？

#### 2. 第 2 回 TOSM ポストの質問

- (a) 正方形を縦横に並べて大きい正方形を作るとき、大小取り混ぜて多くの正方形ができる。 $n$  倍にしたときにできる正方形の数は分かるが、同じことを正三角形でしたら幾つになるか、公式があるか？

- (b) 三角形の辺上の点を通り、三角形の面積を 2 等分する直線を引く問題は中学の教科書にあるが、最初に与える点が辺の上にない場合にも出来るのか？
- (c) 1. 新しいカリキュラムに向かって、数学の目的は何なのか。どう設定するのがいいか。  
2. ほとんどの生徒が文科系を志望しているので、1 年、2 年と学年が進むにつれ実力テストなどで成績が下がる。数学が好きになるような興味付けは出来ないか。

### 3. 第 3 回 TOSM ポストの質問

- (a) 高校数学で、数学的帰納法を  $n \geq 0$  ( $n$  は整数) に対して証明する時、第 1 段を  $n = 0$  で示して第 2 段を  $n \geq k$  ( $k \geq 0$ ) に対して示して良いのでしょうか。それとも、高校では帰納法は自然数である  $n$  に対するものなので、第 1 段で  $n = 0, 1$  に対して示し、第 2 段を  $n \geq k$  ( $k \geq 1$ ) に対して示した方が良いでしょうか。
- (b) 長方形の縦と横はどうして決めるのですか。倒せば縦と横が変わりますし、斜めに置いたら、縦と横とをどうして決めたら良いのでしょうか。(円錐の場合などは、倒しても高さは変わらないのですが、長方形だと変わるような気がします。)
- (c) 円を投影したら何になるか。楕円になると思うが、元の円が内接する正方形を考えて、その投影が台形になる場合に、相対する接点を結ぶ線分の交点は一体何になるのか。

### 4. 第 4 回 TOSM ポストの質問

- (a) ハノイの塔の柱が 4 本になったらどうなるのか？
- (b) 空集合の記号  $\emptyset$  はどう読むのですか。ギリシャ語のファイではないということですが。
- (c) 対偶が真だということと背理法は違うのだという話がありますが、本当はどういうことなのでしょう。

第 1-3 回の分についてはこれまでの会誌 [3], [4] に解説を述べてありますので、第 4 回の質問についてだけ以下でコメントと解答をすることにします。

æ æ

## 2.2 ハノイの塔の柱が4本になったらどうなるのか？

### 2.2.1 ハノイの塔とは

元は仏教説話の中で、世界の終わりまでの時間を表す為に提出されたもののようであるが、出典となる仏典が何なのかは知らない。

今も三重の塔や五重の塔、さらには十三重の塔で見られるように、舍利塔は上の方ほど小さいが、同じ造りの構造物が層のように積み上げられている。

ある仮想的な場所に三基の塔が建っている。ただし、すべての層が積み上げられた完成品は一つだけで、他の塔には一つの層も積まれていない。今ひとつの世界が完全な姿で存在するという気持ちだろうか。

各層は自由に取り外しが出来、別の塔にすべての層を移し変えようとする神か仏かが居る。妖精だと思っ方が楽しければそれでも良い。上に位置する層は下層より小さいので、移し変える際に大きな層の下にならない様にしなければならない。

層の数は  $64 = 2^6$  だったと思うが、それだと仮令一つの層を移し変えるのに1秒しか掛からなかったとしても、すべて移し変えるのに必要な時間は我々が知っている宇宙の年齢をはるかに越えてしまう。古代インド人の想像力の凄まじさ。

現在のハノイの塔は、19世紀ヨーロッパのある数学パズラーが、教育用具としてか単なるゲームとしてか考案したものである。3本の棒を打ち立て、その棒の太さより少し広い穴を中心に持つ薄い円盤を用意する。円盤の半径はすべて異なり、その大きさは等差数列をなすようにしておく。すべて色を変えた実物を見たことがあるが、大小の区別をしやすいのが良いのだろう。

1本の棒にすべての穴開き板(円盤)を大きさの順に差し込んで、さあスタートである。で、どうすれば良いのだろう？

どれか別の棒に移し変えるだけなら、試行錯誤しているうちに出来ることもあるだろうし、ゲームとしてはそれで良いのかもしれない。

数学で取り扱うとなると、何が出来たとしたら許されるのかをはっきりさせておかなければならない。

円盤の枚数が幾つであっても移し変えることが出来るとか、その場合の最短手順の回数とか、またその手順を見つける方法が分かれば良いとも言えるだろう(これが決まっていと、「4本になったらどうなるのか？」という質問にどう答えたら良いか分からない)。

その問題も込めてこれから考えてみるのだが、考えてみるほど塔の数が3であることの素晴らしさが分かってくる。4以上とは本質的に違うのである。泣き言を言っても始まらない。数学は結果より、その解答に至ろうとするアプローチのあり方こそが重要だという言い訳を用意しながら先へ進むことにしよう。

### 2.2.2 ハノイの塔の状態の表し方

ハノイの塔の円盤を移していく途中の状態を、きちんと表現しておかなくてはいけない。それには大きく分けて、二つの方法がある。

できるだけ一般に考えてみる。円盤の数は  $n(\geq 1)$  枚、棒の数は  $k(\geq 3)$  本であるとする。

円盤には小さい方から大きい方に向かって1から  $n$  までの番号をつけ、棒には適当に1から  $k$  までの番号をつけておこう。つまり、円盤は  $I_n = \{1, 2, 3, \dots, n\}$  の元で表される。棒も  $I_k$  の元で表されるが、混同をさける為に同じものだが  $J_k$  と表すことにしておこう。

1. 各々の棒にどれだけの円盤があるのかを指定する方法。

数学的には、 $I_n$  を  $k$  個の部分集合の離散和に分けることで、各  $i$  番目の棒にどれだけの円盤があるのかを指定するということになる。それぞれの棒では、小さい円盤が大きい円盤の上に来るように規制しているので、 $I_n$  の部分集合  $f(i)$  を取るだけで指定できる。つまり、状態を表す集合は、

$$Hanoi_n^k = \{f : J_k \longrightarrow 2^{I_n} = \mathcal{P}(I_n) \mid f(i) \cap f(j) = \emptyset (i \neq j), \cup_{i=1}^k f(i) = I_n\}$$

となる。またこの元  $f$  はその像を並べたもの  $(f(1), f(2), \dots, f(k))$  と表現することもできる。もちろん、 $2^{I_n} = \mathcal{P}(I_n)$  は  $I_n$  の巾集合、つまり、 $I_n$  のすべての部分集合のなす集合である。

すると、最初の状態は  $f_1 = (I_n, \underbrace{\emptyset, \emptyset, \dots, \emptyset}_{n-1})$  となる。これを例えば  $f_2 = (\emptyset, I_n, \underbrace{\emptyset, \dots, \emptyset}_{n-2})$  という状態に移行させればよい。

状態  $f$  にあるハノイの塔の円盤の移動は、 $f(i)$  の最小の円盤が  $f(j)$  の最小の円盤より小さいときに限り、 $f(i)$  の最小の円盤を  $f(j)$  に動かすことが出来るという規則にしたがって動かすことになる。ただし、 $\emptyset$  には円盤がないのだから最小の円盤もないわけだが、最小の円盤の大きさを  $n+1$  としておけば、 $\emptyset$  の場合にも上の規則で動かせば良いことになる。この規約は円盤のない棒にはどんな大きさの円盤も移すことが出来るし、存在しない円盤は移すことが出来ないという事情を反映している。

この表示は視覚的で分かり易く、例えば、 $n = 9, k = 5$  の場合で  $(\{1\}, \{2, 4, 7, 9\}, \{3, 6\}, \{5, 8\}, \emptyset)$  という状態であったとすれば、直ちに次の図表を連想でき、実際のハノイの塔の状態も想像が出来るだろう。紙の上に経済的に書き表そうと思えば、こうする以上に分かりやすい方法は思い付かない。

	2				
	4				
	7	3	5		
1	9	6	8		
1	2	3	4	5	棒

しかし、円盤の移動は、 $k$  個の集合の最小元を取って、それらを比べることになり(最大  ${}_n C_2$  回) 簡潔かつ機能的に表現することが難しく、移動状況の数学的表現は単純とは言い難い。

## 2. 各円盤が何番目の棒にあるかを表わす方法。

円盤  $i$  がある棒の番号が指定されれば良いのだから、ハノイの塔の状態は  $I_n$  から  $J_k$  への写像として表すことが出来る。つまり状態を表す集合は、

$$Hanoi_n^k = \{\phi : I_n \longrightarrow J_k\} = \{(x_1, x_2, \dots, x_n) \mid x_i \in J_k\} = J_k^n$$

で、この表示から  $k$  本  $n$  枚のハノイの塔には  $k^n$  種類の状態があることが分かる。

1 番目の棒にすべての円盤がある最初の状態は  $1^n (= \underbrace{111 \dots 1}_n) = (1, 1, 1, \dots, 1)$  と書かれる。これを、例えば  $2^n (= \underbrace{222 \dots 2}_n) = (2, 2, \dots, 2)$  に変えるのである。

円盤  $i$  の移動は、 $i$  番目の数  $\phi(i)$  を変更することで表現される。ある数 (棒を表している) が左から見て最初に現れる円盤を動かすことが出来るが (その数を変えるということ) それより前の場所に現れている数に変えることは出来ない、という規則にしたがって動かすのである。言いかえると、各々の数  $i \in J_k$  のうち一番前に位置するものだけが変えられるのだが、 $j$  に変えることの出来るのはその位置より前に  $j$  が存在しないときに限るということである。

例えば、 $n = 9, k = 5$  の場合で 123243242 とすれば (括弧とコンマを取って表せばずっと簡単に見える。もちろん  $k \leq 9$  までしか駄目だが) 第 1 の方法の例と同じになる。1 は 1 番目にしかないから、1 番の棒には 1 番の円盤しかないことを意味する。2 が 2, 4, 7, 9 番目にあるから、2 番の棒には 2, 4, 7, 9 番目の円盤がこの順で上から重なっていることを、3 が 3, 6 番目にあるから 3 番の棒には 3, 6 番目の円盤が、4 が 5, 8 番目にあるから、4 番の棒には 5, 8 番目の円盤が、5 はどこにもないから 5 番の棒には円盤がないことを意味している。

上の表を見ながら納得して下さい。動かし方の例も挙げておく。例えば 3 を変えようとすると一番左にある 3 番目のものしか変えられない。これは、3 番目の棒にある円盤で動かせるのは一番上の円盤 3 だけで、円盤 5 は動かさないことを意味する。また、変えることの出来る数が 4, 5 だけであるのは、1, 2 番目の棒にはより小さな円盤があるので、その上へは移動できないということの意味する。

$n$  が小さいときなら、1 番目の表示は状態も移動も、視覚的な分かり易くて良いのだが、 $n$  が大きくなっていくといちいち書くのが煩雑で、2 番目の表示の方が役に立つことが分かる。

### 2.2.3 ハノイの塔の最短手順

$k$  本  $n$  枚のハノイの塔で、一つの塔から別の塔へ移し変えるがあれば、その中での最短手順の回数を  $a_n^k$  と書こう。数学的にキチンと言うとすると、最短手順があるとすればということになるが、それにはどんな手順でもいいから有限回の手順で移し変えることが出来れば良いのだから、あまり気にしなくても良い。どうしても気になるというなら、移しかえることが出来ない場合には  $\infty$  とすることにしておけば良い。実は、下で見るように

$a_n^k \leq a_n^3$  であり、 $a_n^3 = 2^n - 1$  であるから、 $k$  本の  $n$  枚のハノイの塔での最短手順は保証されており、 $a_n^k$  は有限の自然数であることが分かる。

すぐに分かることを挙げておく。

- $a_1^k = 1$  (1枚ならいつでも1回で移せるということ)
- $k \geq h$  なら  $a_n^k \leq a_n^h$  (枚数が同じなら塔が多い方が移しやすい)
- $k > n$  なら  $a_n^k = 2n - 1$  (塔の数が円盤の枚数より多ければ、移しかえる過程で、どの塔に移していけないという制約がないから(自由移動と呼ぼう))

3本ハノイ ( $k = 3$  の場合) が何故特別かということを見ておこう。一般の  $n$  の場合の主張を示そうとすれば、直ちに見て取れる場合を除けば数学的帰納法に訴えるしか、ほかの方法はないといって良い。つまり、何らかの形で  $n - 1$  の場合に帰着できれば有り難いし、そうでなくても、 $n - 2$  以下の有限の状況の組み合わせに帰着できないと困るのである。 $k = 3$  のときはこれが可能だが、 $k \geq 4$  ではうまく方法が見つからなくて弱っている。

$k = 3$  とし初期状態は  $1^n \in \text{Hanoi}_n^3$  であるとする。ここで、一番下の円盤を動かそうとするとき可能な状況を考えて、 $2^{n-1} = \underbrace{22 \cdots 2}_{n-1} 1$  か  $3^{n-1} 1$  のいずれかしか有り得ない<sup>3</sup>。

面倒なので、 $a_n = a_n^3$  と書き、今は  $3^{n-1} 1$  に移したとする。 $1^n$  から  $3^{n-1} 1$  にいたる手順は  $\text{Hanoi}_{n-1}^3$  での最短手順 (回数は  $a_{n-1}$ ) を施すのが最善である。そこで、円盤  $n$  を棒 2 に移し ( $3^{n-2}$  に変えるということ)、棒 3 にある  $n - 1$  枚の円盤を  $\text{Hanoi}_{n-1}^3$  での最短手順で棒 2 に移せば良い。

これによって、次の漸化式が得られる。

$$a_n = 2a_{n-1} + 1$$

$a_1 = 1$  の初期条件でこの漸化式を解けば、 $a_n = 2^n - 1$  となることは高校数学の定石である ( $a_n + 1 = 2(a_{n-1} + 1) = \cdots = 2^{n-1}(a_1 + 1) = 2^n$ )。

この解き方から、再帰的に、最短手順のアルゴリズムを得るにはどうしたら良いかもすぐに分かる。

しかし、 $k \geq 4$  となると事情が異なってくる。

$k > n$  なら  $a_n^k = 2n - 1$  であるが、 $n \geq k$  の時はどうなるか分からない。しかし、ここまでのことから、次の漸化不等式なら得られる。まず  $n + 2 - k$  枚の円盤を最短手順で  $n$  番目の棒に移す ( $a_{n+2-k}^k$  回) と、残った  $k - 2$  枚は  $2(k - 2) - 1$  回で 2 番目の棒に移すことが出来 (自由移動)、 $n$  番目の棒にある  $n + 2 - k$  枚の円盤を最短手順で 2 番目の棒に移せば良い ( $a_{n+2-k}^k$  回)。したがって

$$a_n^k \leq 2a_{n+2-k}^k + 2k - 5$$

<sup>3</sup> 一番右の 1 を変えようとするに左に 1 があってはいけないし、変えることが出来る数は 2 か 3 かしかないのだが ( $k = 3$  だから)、2 と 3 がともに左にあれば 1 を変えることが出来ないから

を得る。4本  $n$  枚ハノイの最短回数  $b_n = a_n^4$  に対しては

$$b_n \leq 2b_{n-2} + 3$$

となり、初期値  $b_1 = 1, b_2 = 3$  に注意すれば、3本ハノイのときと同様に、 $b_n + 3 = 2(b_{n-2} + 3)$  から、

$$b_{2n-1} \leq 2^{n+1} - 3, \quad b_{2n} \leq 3 \times (2^n - 1)$$

という評価を得る。これを第1次評価と呼ぼう。こうして、オーダーとしては4本ハノイの最短手順は3本ハノイの手順数  $a_n = 2^n - 1$  の平方根よりも小さくなるのが分かる。

しかし、この評価は更にずっと良くなる。以下の議論も最短を与えるものとは言えないが、驚くほど評価は良くなる。上の第1次評価は、下の議論で  $b_n(n-2)$  で  $b_n$  を評価していることにあたっている。

$1 \leq \ell \leq n-1$  枚だけ4本ハノイの最短手段で動かし ( $b_\ell$  回)、動かした先に触れずに、3本ハノイで残りの  $n-\ell$  を動かし ( $a_{n-\ell}$  回)、また  $\ell$  枚の4本ハノイで動かして、 $n$  枚の4本ハノイを得る手段の回数を  $b_n(\ell) = 2b_\ell + a_{n-\ell}$  と置けば、 $b_n \leq \min_{1 \leq \ell \leq n-1} b_n(\ell)$  である。これを第2次評価と呼ぼう。

図式的に描いておくと、

$$1^n \xrightarrow{b_\ell} 4^\ell 1^{n-\ell} \xrightarrow{a_{n-\ell}} 4^\ell 2^{n-\ell} \xrightarrow{b_\ell} 2^n$$

という手順を踏むことになる。 $\implies$  は4本ハノイの手順で、 $\longrightarrow$  は3本ハノイの手順で行うことになる。 $\ell$  を動かしたときの最小のものを第2次評価としているのである。 $a_2 = 3$  は自由移動に当たっていて、真ん中の過程を自由移動にするのを第1次評価としているのであった。

$n$  の小さいところで少し計算してみると、次のようになる。

$$b_1 = 1$$

$$b_2 = 3$$

$$b_3 = 5 \quad (\text{ここまでは } k = 4 > n = 3 \text{ の場合にあたる})$$

$$b_4 = 9; b_4 \leq b_4(1) = 2b_1 + a_3 = 2 \times 1 + 7 = 9$$

$$b_4(2) = 2b_2 + a_2 = 2 \times 3 + 3 = 9$$

$$b_4(3) = 2b_3 + a_1 = 2 \times 5 + 1 = 11$$

$$b_5 \leq 13 = 13; b_5 \leq b_5(1) = 2b_1 + a_4 = 2 \times 1 + 15 = 17$$

$$b_5(2) = 2b_2 + a_3 = 2 \times 3 + 7 = 13$$

$$b_5(3) = 2b_3 + a_2 = 2 \times 5 + 3 = 13$$

$$b_5(4) = 2b_4 + a_1 = 2 \times 9 + 1 = 19$$

$$b_6 \leq 17 < 21; b_6 \leq b_6(1) = 2b_1 + a_5 = 2 \times 1 + 31 = 35$$

$$b_6(2) = 2b_2 + a_4 = 2 \times 3 + 15 = 21$$

$$b_6(3) = 2b_3 + a_3 = 2 \times 5 + 7 = 17$$

$$b_6(4) = 2b_4 + a_2 = 2 \times 9 + 3 = 21$$

$$b_6(5) = 2b_5 + a_1 \leq 2 \times 13 + 1 = 27$$

$$b_7 \leq 25 < 29; b_7 \leq b_7(1) = 2b_1 + a_6 = 2 \times 1 + 63 = 65$$

$$b_7(2) = 2b_2 + a_5 = 2 \times 3 + 31 = 37$$

$$b_7(3) = 2b_3 + a_4 = 2 \times 5 + 15 = 25$$

$$b_7(4) = 2b_4 + a_3 = 2 \times 9 + 7 = 25$$

$$b_7(5) = 2b_5 + a_2 \leq 2 \times 13 + 3 = 29$$

$$b_7(6) = 2b_6 + a_1 \leq 2 \times 17 + 1 = 35$$

第1次評価と比べると、 $n \geq 6$  でやっと差が出てくる。 $b_6 \leq 17$ ,  $b_7 \leq 25$  が得られ、第1次評価より4小さくなっている。更にやってみると  $b_8 \leq 33$  では7、 $b_9 \leq 41$  では20も小さくなる。オーダーに影響するほどかどうかを調べる為に、計算機でこの第2次評価を  $n = 2000$  まで実行してみた<sup>4</sup>、

$n$	$b_n$ の第2次評価	$b_n$ の第1次評価	$a_n$
10	49	93	1023
20	289	3069	1048575
30	1025	98301	1073741824
40	2817	3145725	1099511627776
50	6657	100663296	1125899906842624
60	14337	3221225469	$1.1529215046847 \times 10^{18}$
70	28673	137438953469	$1.180591620717411 \times 10^{21}$
80	53249	3298534883325	$1.208925819614629 \times 10^{24}$
90	94209	70368744177661	$6.189700196426901 \times 10^{26}$
100	172033	3377699720527869	$1.267650600228229 \times 10^{30}$
(103	196609	9007199254740989	$1.014120480182584 \times 10^{31}$ )
200	14680065	$3.802951800684688 \times 10^{30}$	$1.606938044258990 \times 10^{60}$
300	385875968	$4.28174307811788 \times 10^{45}$	$2.037035976334486 \times 10^{90}$
400	6445750944	$4.820814132776971 \times 10^{60}$	$2.582249878086909 \times 10^{120}$
500	73014444032	$5.427754182999197 \times 10^{75}$	$3.273390607896142 \times 10^{150}$
600	652835028992	$6.111107929003458 \times 10^{90}$	$4.149515568880993 \times 10^{180}$
700	4741643894784	$6.880495847970215 \times 10^{105}$	$5.260135901548374 \times 10^{210}$
800	31885837205504	$7.746749634260726 \times 10^{120}$	$6.668014432879854 \times 10^{240}$
900	173722837188608	$8.722064691547283 \times 10^{135}$	$8.452712498170644 \times 10^{270}$
1000	932385860354049	$9.820171823688426 \times 10^{150}$	$1.071508607186267 \times 10^{301}$
2000	$4.980620899901579 \times 10^{20}$	$3.214525821558802 \times 10^{301}$	

となった。第2次評価の定義式から、小さくなることは分かっていたが、これほどとは思わなかった。

2番目の表示を使って、具体的な手を探して行きながら、この差の意味を考えていくという実験も出来るし、時間があればやってみようと思っているが<sup>5</sup>、一般の  $n$  で出来るかどうかの見通しは明るくない。

<sup>4</sup> 使用した処理系では  $n = 104$  で第1次評価が整数表示されなくなり、 $n = 2001$  で第1次評価が、 $n = 1001$  で  $a_n$  の値がオーバーフローした。

<sup>5</sup> 締め切りに追われていて中途半端になりそうです。

本来、円盤を移すという作業にとって、棒（塔）が多ければそれだけやり易くなる。2本のときは、1枚しか移すことが出来ない。3本のときが、任意枚数の円盤を移せる最小の棒の数であって、それ故にこそ、選択の自由が減少し、整然とした構造が顕れてくるのである。数学は一般に、このように自由度の大きい場合を取り扱うのは得意でない。数学者の心情として、出来る限り必要十分で押し進めたいが、自由度が増せば必然性が減少するというせいであろうか。

実験をする前に、一般の  $k > 3$  の場合の第1次評価も見て置くことにしよう。初期条件は自由移動の  $a_\ell = 2\ell - 1$  ( $1 \leq \ell < k$ ) とすれば良く、漸化不等式の形から  $a_n^k + 2k - 5 \leq 2(a_{n+2-k}^k + 2k - 5)$  が得られ、それから  $k - 2$  を法として異なる評価式

$$\begin{aligned} a_{m(k-2)+\ell}^k &\leq 2^m(2k - 5) + 5 - 2k & (\ell = 0) \\ &\leq 2^{m+1}(\ell + k - 3) + 5 - 2k & (1 \leq \ell \leq k - 3) \end{aligned}$$

が得られる<sup>6</sup>。これを3本八ノイのときの値  $a_{m(k-2)+\ell} = 2^{m(k-2)+\ell} - 1$  と比べると、枚数が多くなれば、 $k - 2$  乗根のオーダーでは押さえられることが分かる。

$k = 5$  の場合の第1次評価でも、 $k = 4$  の第2次評価よりはるかに小さくなるので、第1次評価だけの議論は意味がないとも言えるが、ほかに一般的に述べられることが見つからない。

$k = 5$  の場合の第2次評価は、 $k = 4$  の時の説明から分かるように、

$$a_n^k \leq \min_{1 \leq \ell \leq n-1} (2a_{n-\ell}^k + a_\ell^{k-1})$$

という不等式で得られる。 $a_\ell^{k-1}$  が自由移動を表している最大の  $\ell = k - 2$  の値だけで評価したものが第1次評価である。 $Hanoi_n^k$  の元の記述が有効な  $k \leq 9$  に対して、 $n \leq 2000$  まで第1次評価と第2次評価の計算をしてみた。 $n = 50, 100, 500, 1000, 2000$  の時の値を表にして、挙げておく<sup>7</sup>。

$k$	$a_{50}^k$ の第2次評価	$a_{50}^k$ の第1次評価
3	1125899906842624	1125899906842624
4	6657	100663296
5	831	524283
6	449	40953
7	303	9207
8	273	3573
9	239	1779

<sup>6</sup> ここでも、 $k = 3$  すなわち  $k - 2 = 1$  であることが特別なことが分かるだろう。

<sup>7</sup> もしかすると、第2次評価の値もまた最短手順の回数も、何か意味のある組み合わせ論的な数になっているのかもしれない。

$k$	$a_{100}^k$ の第2次評価	$a_{100}^k$ の第1次評価
3	$1.267650600228229 \times 10^{30}$	$1.267650600228229 \times 10^{30}$
4	172033	3377699720527869
5	4863	51539607547
6	1749	234881017
7	1055	9437175
8	801	1179637
9	639	262131

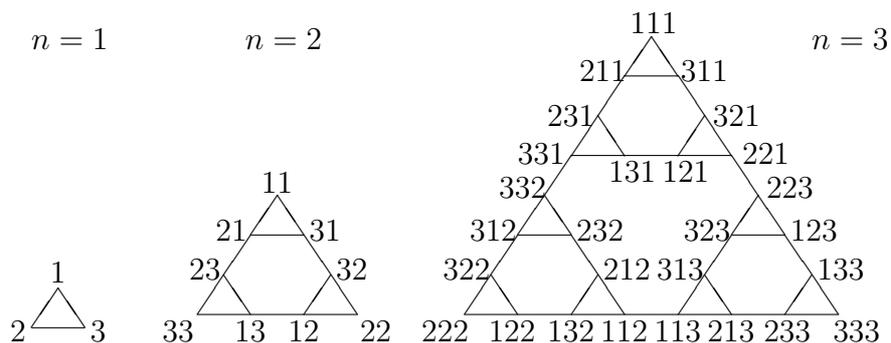
$k$	$a_{500}^k$ の第2次評価	$a_{500}^k$ の第1次評価
3	$3.273390607896142 \times 10^{150}$	$3.273390607896142 \times 10^{150}$
4	73014444032	$5.427754182999197 \times 10^{75}$
5	1015807	$7.482888383134223 \times 10^{50}$
6	68097	$2.977470710558212 \times 10^{38}$
7	23807	$1.140885540205406 \times 10^{31}$
8	13057	$1.353996917968385 \times 10^{26}$
9	9599	$4.250129834582682 \times 10^{22}$

$k$	$a_{1000}^k$ の第2次評価	$a_{1000}^k$ の第1次評価
3	$1.071508607186267 \times 10^{301}$	$1.071508607186267 \times 10^{301}$
4	932385860354049	$9.820171823688426 \times 10^{150}$
5	22020095	$1.049880347895846 \times 10^{101}$
6	470017	$1.266475976033146 \times 10^{76}$
7	114431	$1.446244239833091 \times 10^{61}$
8	49921	$1.683649886205200 \times 10^{51}$
9	32255	$1.338044711911838 \times 10^{44}$

$k$	$a_{2000}^k$ の第2次評価	$a_{2000}^k$ の第1次評価
4	$4.980620899901579 \times 10^{20}$	$3.214525821558802 \times 10^{301}$
5	922746879	$2.449441655328671 \times 10^{201}$
6	4554753	$2.291373425527299 \times 10^{151}$
7	552959	$2.324024890278217 \times 10^{121}$
8	214273	$2.449720811756973 \times 10^{101}$
9	114431	$1.367638900126913 \times 10^{87}$

#### 2.2.4 具体的な手順の例

$1^n$  からどれかの  $i^n$  ( $1 \leq i \leq k$ ) へ移す手順の例を挙げる。( )の中は手順数である。  
 $k = 3$  の場合。この場合は第1次評価の漸化式の要請する最短手順になっている。  
 $n = 1$  のとき、 $1 - 2(1)$



$n = 2$  のとき、 $11 - 21 - 23 - 33$  (3)  
 $n = 3$  のとき、 $111 - 211 - 231 - 331 - 332 - 132 - 122 - 222$  (7)  
 $n = 4$  のとき、 $1111 - 2111 - 2311 - 3311 - 3321 - 1321 - 1221 - 2221 - 2223 - 3223 - 3123 - 1123 - 1133 - 2133 - 2333 - 3333$  (15)  
 $n = 5$  のとき、 $11111 - 21111 - 23111 - 33111 - 33211 - 13211 - 12211 - 22211 - 22231 - 32231 - 31231 - 11231 - 11331 - 21331 - 23331 - 33331 - 33332 - 13332 - 12332 - 22332 - 22132 - 32132 - 31132 - 11132 - 11122 - 21122 - 23122 - 33122 - 33222 - 13222 - 12222 - 22222$  (31)

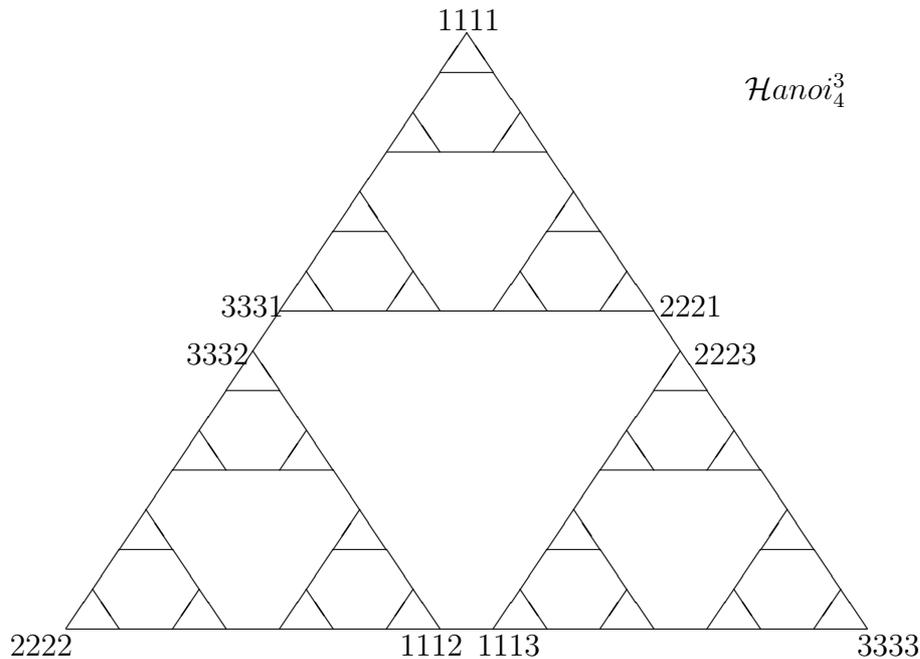
どこでも半分までは一つ上の手順の各項の最後尾に 1 をつけたものになっており、最後尾の 1 を 2 か 3 に変えてから、数字は異なるが前半と同じ構造の手順を行っていることが分かるだろう。

3本ハノイの状態集合  $Hanoi_n^3$  で、各状態を頂点、直接変化させることが出来る状態同士を線分で結べばグラフが得られる。すると、3本ハノイの状態集合  $Hanoi_n^3$  には非常に整然とした構造が見えてくる。まず、 $Hanoi_1^3$  は正三角形になる。次に、 $Hanoi_2^3$  は正三角形の頂点に、 $Hanoi_1^3$  と同型な正三角形が置かれる形になる。同様に、 $Hanoi_n^3$  は正三角形の頂点に、 $Hanoi_{n-1}^3$  と同型なグラフが置かれる形になる。 $1^n, 2^n, 3^n$  はその一番大きな正三角形の頂点にあり、最短経路は正三角形の辺を通るものとなることが分かる。

まず、 $n = 1, 2, 3$  の場合に状態集合  $Hanoi_n^3$  のグラフを描いてみると、  
 となる。 $n = 1$  のグラフの頂点すべての右端に 1 を加えたものが  $n = 2$  のグラフの上部に、さらに  $n = 2$  のグラフの頂点すべての右端に 1 を加えたものが  $n = 3$  のグラフの上部にあることが分かる。

同様に  $n = 3$  のグラフの頂点すべての右端に 1 を加えたものが、以下に描いた  $n = 4$  のグラフの上部にあるが、繁雑になるのですべての頂点の名前を書き込んでいない。演習として残しておく。

$Hanoi_n^3$  を描くときは、 $Hanoi_{n-1}^3$  を 3 つ同じものを描いて、それぞれを 1, 2, 3 の島だと思い、各頂点の名前の右端に島の名前を付け足す。1 の島を上部に置き、2 の島は  $\pm 120^\circ$  回して  $n$  が奇数のときは左下に、 $n$  が偶数のときは右下に置く。回転する方向は  $3^{n-1}2$  が正三角形の上の頂点に来るようにして、頂点  $3^{n-1}2$  と  $3^{n-1}1$  を線で結ぶ。3 の島も同様にしておいた後で、残った 2 頂点  $1^{n-1}2$  と  $1^{n-1}3$  との間の線分をひけば良い。



これ以上詳しい議論はもう止めて、イアン・スチュアートの「おもしろ数学入門」[10]を引用しておこう。 $n$ が大きくなると、グラフはフラクタルの一種であるシェルピンスキーの三角形に似たものになってくる。実際に  $n \rightarrow \infty$  の極限でシェルピンスキーの三角形になることを利用して、シェルピンスキーの三角形の2点間の平均距離をハノイの塔の2状態間の平均手順数の計算から求めた数学者もいる。

$k \geq 4$  のときには、この構造を一言で言い切ることが出来ていない。

$k = 4$  の場合に  $n$  の小さい所で見ると、 $Hanoi_1^4$  は正四面体グラフになるが、そのあとも正四面体の各頂点に一つ小さなものが配置されていくようになっていけば嬉しいのだが、思わぬ所が結ばれて簡単に言い切ることが出来ていない(下図参照)。

$Hanoi_2^4$  は4つの  $Hanoi_1^4$  を用意して、1, 2, 3, 4 と島の名前を付けて、1の島を真ん中に置き、その他の島は正四面体と思って回してみ、適当に1の島の辺と四角形を作るように繋ぐことになっている。

グラフ  $Hanoi_n^4$  の辺で作る最小の多角形は三角形と四角形と交じり合うことになる。 $n = 3$  のグラフをきちんと描けば、何か分かることがあるかもしれないが、今は時間がない。

$k = 3$  のときは平面グラフを与えるが、 $k > 3$  のときは  $n$  が大きくなるとすぐに平面には収まらなくなる。

第1次評価、第2次評価、行き当たりばったりで少しやってみると

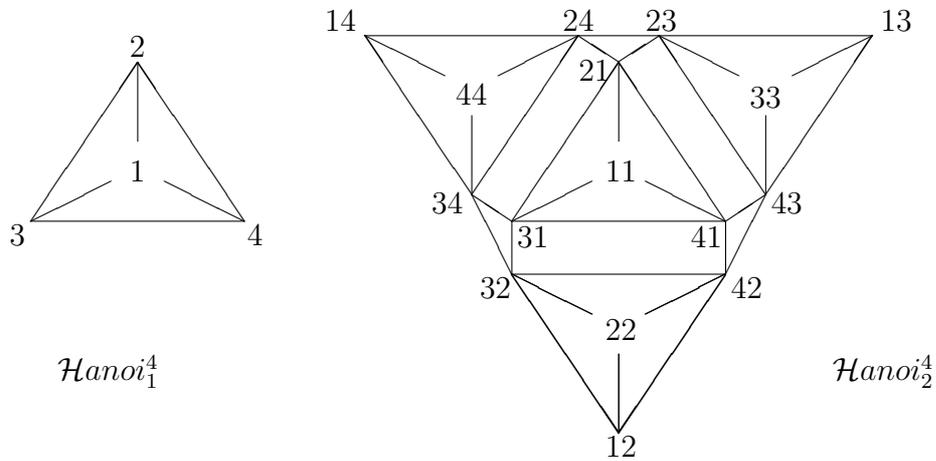
$n = 1$  のとき、1 - 2 (1)

$n = 2$  のとき、11 - 21 - 23 - 33 (3)

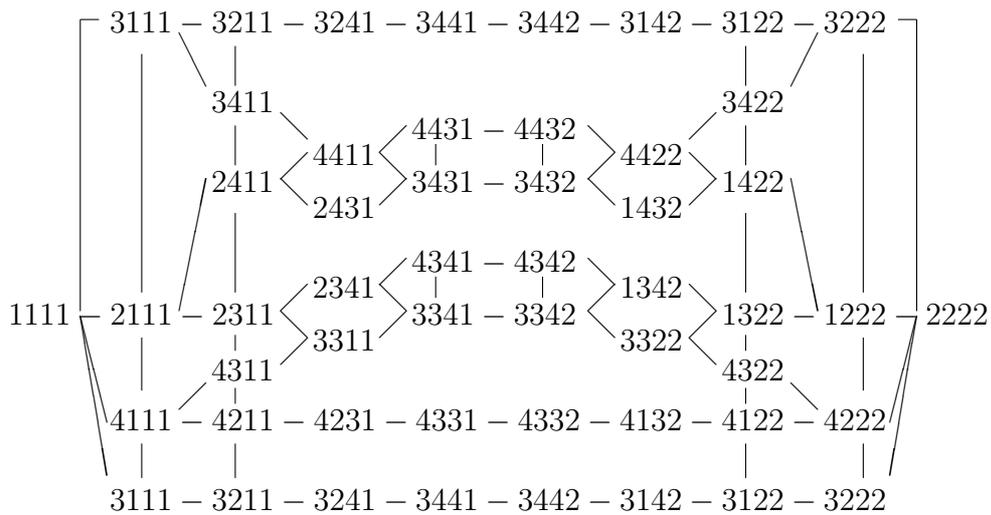
$n = 3$  のとき、111 - 211 - 231 - 234 - 244 - 444 (5)

$n = 4$  のとき、1111 - 2111 - 2311 - 3311 - 3341 - 3342 - 3322 - 1322 - 1222 - 2222 (9)

が第1次評価に即した手続きであるが、少し考えただけでも1111を2222に変える手続きには次のものがある。



$Hanoi_4^4$  において 1111 と 2222 を結ぶ最短の手順



線が重なって見難いので、1番上の列は1番下にもう一度書いてある。1111と2222を最短で結ぶことにかかわるもの以外は、線も頂点も省略してある。それを補ってみると複雑さが実感できると思う。

このグラフの1111と2222を結ぶ最短経路(長さ9)が最短手順を与えていると思うが、ざっと数えただけでも20はある。こんなに自由度が多いと、最短手順の中から特別なものを定性的な言葉で取り出すことが難しい。

以下は少しやってみただけ。これ位のことでは、第2次評価のときもそれを与えるアルゴリズムに特徴的な頂点を、全く通らなくても同じ回数で実現できる例があるのだから、恐らく $n$ が大きくなれば第2次評価よりも短い手順があるだろう、ということぐらいしか分からない。

$n = 5$ のとき、11111-21111-23111-23411-24411-24431-34431-34432-14432-14422-13422-13222-12222-22222 (13)

$n = 5$ のとき、11111-21111-23111-23411-24411-44411-44431-44432-44422-14422-13422-13222-12222-22222 (13) 第1次評価

$n = 6$ のとき、111111-211111-231111-234111-244111-244311-444311-444321-444221-444223-444123-444133-444333-244333-241333-243333-233333-333333 (17)

$n = 6$ のとき、111111-211111-231111-234111-244111-444111-444211-444231-444331-444332-444312-444322-444222-144222-134222-132222-122222-222222 (17)

第2次評価

$n = 6$ のとき、111111-211111-231111-331111-334111-334211-332211-132211-122211-222211-222231-222234-222244-122244-132244-332244-331244-331444-334444-134444-144444-444444 (21) 第1次評価

もう少し大きな $n$ でやらないと、第2次評価が最短を与えていない場合があることを示すことも出来ない。

これらをいつまで手だけでやっても見通しが見つからないので、コンピュータで応答式に支援するプログラムを作ってみようと思っている。少し教育的な工夫を盛り込めば、小中学校で、また高等学校でも使えるようなものが出来るかもしれないが、これは95年度の卒論を準備している学生のテーマにとって置くことにしたい。うまくいけば、使っただけのものが出るかもしれません。

いろいろ書くべきこともありますがこの辺で勘弁していただくことにします。

æ

## 2.3 空集合の記号の読み方

空集合の記号  $\emptyset$  をどう読んだら良いかということですが、まずギリシャ語のファイと違うことを見ておきましょう。

この文章は L<sup>A</sup>T<sub>E</sub>X という組み版ソフトを使って書いているのですが、L<sup>A</sup>T<sub>E</sub>X での印刷上の違いを見てみましょう。命令文そのものと印刷の出来上りを並べてみると

$$\text{空集合} = \backslash\text{emptyset} = \emptyset \quad \text{ギリシャ語のファイ} = \backslash\text{phi} = \phi$$

となって、違っていることは一目瞭然ですね。しかし、違っているということは分かっているの質問でしたから、これでは納得しては頂けないでしょう。

手書きにすれば区別するのが難しいのも、混同しやすい理由でしょう。やはりファイ  $\phi$  とは違うことを意識して、書くときも書いた方が良いでしょう。実際に黒板に  $\phi$  を書いておいて、これはファイ  $\phi$  とは違うのだと言っても、児童・生徒は納得しないでしょう。 $\emptyset$  の書き方としては、数字の 0 を少し大きめに書いてその上に右上方から左下方へ線を引くようなつもりで書くと、 $\phi$  と区別しやすいのではないのでしょうか。

読み方としての結論を先に述べるとすれば、 $\emptyset$  は「空集合」と読むのが良いと思います。

空集合は、上の命令文でも分かるように、英語では empty set です。この頭文字を採って、 $e$  とすれば良いわけですが、 $e$  はアルファベットの前の方にあることもあり、一般に何かの量を表したり、多項式の係数に使ったり、また電荷を表すのにも用いられ、空集合であるというような特徴的な事柄を表すのには適していません。新しい記号が必要です。

どんな集合でも、その要素を一つも含まない部分集合として空集合を持ちます。いろいろな数学的対象からなる集合がありますが、それがどのような対象であっても、その部分集合としての空集合は同じものなのです。つまり、空集合は固有名詞であると言っても良いわけで、見ただけではっきりと分かる記号が欲しかったのです。

アンドレ・ヴェイユの自伝 [11] は、記号が生まれる経緯が語られています。それによれば、ブルバキが「集合論要約」を出す時に集合論で使う記号を整理したり発明したのだそうです。その時ノルウェー語の字母で少し硬い「エ」という音の  $\emptyset$  を使うことにしたようです。その時の会議の場にノルウェー語を知っていたのは自分だけで、だから  $\emptyset$  は自分の発明なんだと、学校で集合論を習って来た小さい娘に自慢できて、ヴェイユはとても嬉しかったということです。

それはともかく、 $\emptyset$  は空集合を表しており、空集合と読むのが適当だと思います。たとえば、ノルウェー語を勉強して正確に発音したとしても、聞いた人がそのことを認識してくれないような音を出して見せても仕方がないと思います。

また、ある人は void と呼んでいるがと質問にありましたが、それは単に、日本語であっても、ある集合が「空集合である」と言わずに、形容詞に変えて、「空(くう)である」と言うことも、「空(から)である」と言うこともあるだろうというくらいのことではありません。

どう読むのかという疑問が単なる好奇心ならそれで良いのですが、どう読まねばならないかというような議論は倫理臭を感じさせない程度にしておくのが良いと思います。どういう概念なのかが問題なので、正々堂々と、「空集合である」と読むのが良いと思います。

## 2.4 対偶による証明法と背理法との違い

対偶を用いた証明法は背理法の一つであるという高校教科書の記述に納得しにくいものを感じているというのが、質問の趣旨のようです。対偶を用いた証明法で背理法を示すことができるのではという疑問もありました。背理法による証明を対偶を証明する方法であると誤解しないようにという記事を引用して、その方向で考えたいがという思いも書かれていました。

これらの質問に答える為には背理法とは何か、また対偶とは何かをはっきりさせておく必要があります。さらに、真理値とは何かということも問題になります。実は、仮題「小学校教師の数学的常識」という教科書を何年か前から書き始めていて、その論理についての節に少し詳しい議論があります。その原稿を次節に添付しますので、ここでまずその節を参照して下さい<sup>8</sup>。

背理法の意味を、質問者の添付してくれた高校教科書の記述に従って、「命題  $R$  を否定して矛盾を導くことにより、命題  $R$  の成り立つことを示す」ということにすれば、確かに対偶を用いた証明法は背理法の一つということになります。

教科書の説明は簡単過ぎて納得出来ないことがあっても仕方が無いかもしれませんが、素直にその記述のままに納得しておいた方が「幸せ」かも知れません。きちんと納得したいという質問なので、次節を読んでいるという前提のもとに、少し細かい議論を試みますが、分かりやすいとは言えないと思います。これは、事柄がかなり微妙で根源的な問題を含んでいるので、一般的にするこのような議論では、止むを得ないことも了解しておいて下さい。

質問者の添付した文章には、 $P \implies Q$  をその対偶  $\neg Q \implies \neg P$  を示すことで証明することと、背理法とは差のあることが指摘してあります。つまり、 $\neg Q$  を仮定して  $\neg P$  を示さなくても、公理、定理、仮定に反することを示せば良いからとあります。

確かにこれはこれで正しいのですが<sup>9</sup>、背理法で示すということの意味を考えてみる必要があります。

「背理法」を広辞苑で引くと、「帰謬法」を見よとあり、「帰謬法」を引くと *reductio ad absurdum* (ラテン語) とあって、「否定命題  $\neg P$  を仮に真とすれば結局不条理に陥ることを示して命題  $P$  が真であることを間接的に証明する方法」であるとなっています。ラテン語もその直訳である帰謬法という術語もこの定義をよく表していると思いますが、恐らくは「謬」という文字を避けるために造語された「背理法」という術語は少しニュアンスが違うようです。この差がまた、混乱の元なのかもしれません。

問題はこの「不条理」ということなのです。不条理とは何にとって不条理か、また不条理とは一体どういうことか、が問題なのです。次節を読むと、意味のはっきりしない宇宙と呼ばれる集合  $\Omega$  が何故かとても重要なもののように感じられないでしょうか。そう感じ

<sup>8</sup> 何人かの学生にこの部分を読ませてみた所、次節を読んだからとここに書いてあるにも拘わらず、次節を読まずに以下を読み進み、意味が判らんと不平を言います。ぜひ次節を先にお読みください。まだ出ていない本の宣伝をしているわけではありません。

<sup>9</sup> 正しいかどうかを問題にするのではなく、教育上の技術的な提言だと思った方が良いのではないのでしょうか。つまり、 $\neg Q$  が真であると仮定したとき、ひたすら  $\neg P$  を示そうとするのではなく、公理にでも、定理にでも、定義にでも何でもいから矛盾を導けばいいという指導の方が、生徒の気持ちは少しでも自由になれるのではないのでしょうか。

てもらえれば良かったのです。命題  $P$  の真理値とは  $\Omega$  の元  $x$  に対して、 $P(x)$  が真であるか偽であるかを与えるものなのです。「命題  $\neg P$  を仮に真とすれば」ということは、 $P(x)$  が偽であるような  $x \in \Omega$  を考えれば、ということであり、不条理というのは、そのように仮定したとき  $x$  は  $\Omega$  の元であるために守るべき規範に反しているということなのです。

それでもなお気持ちが悪ければ、 $\Omega$  を含む十分大きな集合  $\tilde{\Omega}$ <sup>10</sup> を考え、 $x$  は  $\tilde{\Omega}$  の元だと思っておき、 $P(x)$  が偽であると仮定すれば、 $x$  はもはや  $\Omega$  にはいられない ( $x \in \tilde{\Omega} \setminus \Omega$ ) ことが示されるということにすればいい。そのためには、 $\tilde{\Omega}$  の中で部分集合  $\Omega$  を特徴付けている条件や性質（これがこの世界  $\Omega$  における公理や定理に当たる）を満たしていないことを言っても良いのです。

排中律の定式化は、次節によれば、「複合命題  $P(x) \vee \neg P(x)$  は常に真で、 $P(x) \wedge \neg P(x)$  は常に偽である」ことでした。命題  $P$  が真である範囲  $M_P$  も本来は  $M_P = \{x \in \Omega | P(x)\}$  と書くべきであったし、命題  $P$  が偽である範囲  $M_{\neg P}$  は  $M_{\neg P} = \{x \in \Omega | \neg P(x)\}$  となる。この時排中律は、 $M_P \cup M_{\neg P} = \Omega$  かつ  $M_P \cap M_{\neg P} = \emptyset$  であることを意味しています<sup>11</sup>。

宇宙  $\Omega$  の中では、どんな命題  $P$  に対しても、 $P$  が成り立つか  $\neg P$  が成り立つかのいずれか一方だけが成り立つということです。

$\neg P$  が真であると仮定して不条理に陥るとは、 $\neg P(x)$  が真であるような  $x$  は  $\Omega$  の元では有りえないことを示したことになるので、 $M_{\neg P} = \emptyset$  であること、すなわち、 $M_P = \Omega$  であることが示され、つまり宇宙全体で  $P$  が真であることが示されたことになるのです。

これが背理法の意味であり、それは排中律そのものであると言っても良いほど直接的な排中律の帰結だといえるでしょう。

議論が繁雑になるので止めますが、排中律をフルに使えば、真理値の同じ命題は全く同じと考えていることになることに注意しておきます。

さて、問題を仮言命題  $P \implies Q$  を証明することに限って議論してみましょう。

そもそも、この命題の対偶  $\neg Q \implies \neg P$  を示すことによって、何故元の命題  $P \implies Q$  が示されたことになるのでしょうか。

次節を読んで貰っていればこれは明らかなことになっているでしょう。 $P \implies Q$  は  $P, Q$  の複合命題として  $\neg P \vee Q$  と表され、対偶  $\neg Q \implies \neg P$  は  $\neg(\neg Q) \vee \neg P$  と表されるのだが、この二つは論理式としてまったく同等なのですから、対偶を示すこと、すなわち元の命題を示すことだったわけです。

しかし、こんな当たり前のことで良いのでしょうか。

論理式が同じであることを示す変形を見ていると、 $\neg(\neg Q) = Q$  であるという変形がポイントであることが分かるでしょう。

しかし、これこそ上に述べた排中律そのものだと言っても良い事柄なのです。排中律は、理性においては疑うことが出来ないほど明らかで受け入れやすいことなのに、感性においてはなかなか受け入れにくいということがあります。それは往々にして、宇宙  $\Omega$  と拡大宇宙  $\tilde{\Omega}$  とを混同することにあるようですが、これは生徒には説明しにくいでしょう。

少し別の角度から考えてみましょう。

$\neg Q(x)$  が真であると仮定しましょう。

<sup>10</sup> 宇宙  $\Omega$  を銀河系とでも考えたら銀河系集団のようなもの

<sup>11</sup> 分からないという人のために、老婆心ながらもう一度言います。次節を読みましたか？

その時  $\neg P(x)$  が真であることが示されたとすればどういうことになるのでしょうか。そのとき、 $P \implies Q$  が示せたら良いのですね。

それでは  $P(y)$  が真だとしましょう。  $Q(y)$  が真だと主張したいのですが、とにかく排中律から  $Q(y)$  は真か偽かのいずれか一方だけが成り立っているのです。  $Q(y)$  が偽だと仮定したら、  $\neg P(y)$  が真であることが示されているのですから、排中律から  $P(y)$  と  $\neg P(y)$  が共に真であるような元  $y$  は宇宙  $\Omega$  には存在しないことになります。したがって  $Q(y)$  は真でなければならぬことになります。

これはよろしいですね。

さてもう一方の方を考えてみましょう。  $\neg Q(x)$  が真であると仮定して、何らかの公理などとの間に矛盾を起こさせて不条理であることが示されたとします。

しかしそれで、  $P \implies Q$  が示せたことになるのでしょうか。矛盾に導く際に  $P$  であることを一切使わなかったとすれば、それは  $P \implies Q$  などではなく、  $Q(x)$  が  $\Omega$  上どこでも、つまりいつでも  $Q$  が成り立つことを示していることになります。

だからやはり、具体的に現れていなくても何らかの形で、  $P$  を仮定していることになるのです。つまり示したことは、  $P$  と  $\neg Q$  とを仮定して矛盾を導いた、すなわち  $P \wedge \neg Q$  は偽であることが示されたことになり、それは取りも直さず、  $\neg(P \wedge \neg Q) = \neg P \vee Q$  が真であるのです。そしてこの最後の式は  $P \implies Q$  の定義式に他なりません。

結局、  $P \implies Q$  を示す二つの方法は、排中律をどこでどんな形で使うのかが違うだけで本質的には差のないものであることが分かったわけです。

お疲れ様でした。さて、

大山鳴動してネズミ一匹

出たでしょうか。  $\infty$

## 2.5 論理（数学のグラマー）[「小学校教師の数学的常識」より]

アルファベット<sup>12</sup> だけでは言葉にはならない。学ぶには文法も必要である。数学でも集合について何か主張しようと思えば、論理が必要になるのである。

Logic を訳すのに論理という言葉を選んだ人は、議論するときの理屈という面を強調したかったのだろう。その議論とは、命題を一定の規範で並べていかないといけない。議論とは、相手か第三者かを納得させるためのものだから、自分の主張したい命題を連呼しているだけではいけない。共通に納得出来る基盤から、承認できる命題の連鎖で主張したい命題を導く必要がある。論理学は古代ギリシャで生まれた。古代ギリシャは民主的な多民族国家だったが、国家の成立から多くの議論が必要であり、人を説得する技術としての雄弁術が盛んであった。

議論しようとする人々が共通に承認する命題を公理 Axiom と言い、後は三段論法だけを用いて主張したい命題を導くのが最も本格的な議論の仕方であった。基本的にはこれ以外の論理の運用を認めないのは数学だけで、当時は幾何学がその主流であった。プラトンの学塾アカデメイアの入り口に「幾何学を知らざるものこの門に入るを許さず」と書いてあったというが、論理の正しい運用も出来ないものは入学できないという入学の条件だったということかもしれない。

当時の多くの雄弁家はまた詭弁（インチキな議論）の達人でもあって、それが政治の歪みを引き起こし、社会の関心事でもあったのだろう。正しい論理の運用の術が、幾何学をモデルに整備されてゆき、その集大成がプラトンの弟子であるアリストテレスの論理学という本である。これが古典論理学であり、基本的には現在もこれから出るものではない。

正しい論理を知るためには詭弁も知っておく必要がある。アリストテレスには詭弁の分類もあって面白いが、まず命題について考えてみることにしよう。

命題はそれ自体文章なのだが、どんな文章でもよいという訳ではなく、基本的なものの適切な組み合わせだけを考えることにするのである。まず基本的な命題を「 $A$ は $B$ である」という形の文章  $P$  とする。 $B$  として「 $C$ をするもの」とか「 $D$ なもの」を考えることによって、述語に動詞や形容詞を使うことも出来る。

さて、 $A$  が固有名詞なら命題  $P$  も確定した意味を持ち得るが、 $A$  が普通名詞であったりすると曖昧さが残る。例えば「リンゴは赤い」という命題  $P$  を考えて見よう。 $A$  = 「リンゴ」、 $B$  = 「赤い」である。今目の前にしている特定のリンゴという意味でなら別だが、普通は「リンゴ」は普通名詞として考えているだろう。確かにリンゴの多くは赤いけれど、黄色のリンゴも青いリンゴもある。だから  $P$  は正しいとも言えるし、正しくないとも言える。

前の節で集合を  $M = \{a|P(a)\}$  と表わしたが、集合に対する要請として「 $a \in M$ 」か「 $a \notin M$ 」かのどちらかが成り立たねばならなかった。命題  $P$  にとって言えば、 $P$  が真であるか偽であるかのどちらかが成り立たねばならないということになる。

「リンゴは赤い」というのは命題ではないのだろうか？

確かにこのままでは数学的に処理できる命題とは言えない。しかしほとんどの文章はこのようなものである。その本質は変えないで、成り立つか否かが確定するようにするには

<sup>12</sup> 未完の教科書 [9] のこれより前の節で集合は数学のアルファベットであると言って少し集合の話がしてある。以下それを前提とした議論もあるが、ここで理解するのに支障がないと思うのでそのままにしておいた。

どうしたら良いだろうか？

全称命題と特称命題という概念を導入するのである。「リンゴは赤い」というとき、赤いリンゴがそうでないリンゴより多いとか、赤いりんごがリンゴの典型的なものであるとかいう意味であることが多い。しかし、「多い」というのも状況によって変わるかもしれないし、典型というのも人によって変わるかもしれない。青いリンゴしか生らない土地の人には「リンゴは赤い」という命題はとても奇異に感じられるだろう。すべての人に同じように納得してもらうために、主張を百歩譲って「赤いリンゴもある」ということだけにする。「あるリンゴは赤い」とか「赤いリンゴがある」とか言うのであれば、真偽がはっきりするだろう。もちろん、真である。このように「ある  $A$  は  $B$  である」という形なら命題に対する要請を満たす。これを 特称命題 と言う。

これに対して「すべてのリンゴは赤い」というのを 全称命題 と言うのである。明らかに、これは偽であるわけで、真偽が確定しているので命題と呼べるのである。

曖昧に見える「 $A$  は  $B$  である」という文章を、「ある  $A$  は  $B$  である」という特称命題と、「すべての  $A$  は  $B$  である」という全称命題とに分けることにすれば、はっきりと真偽が判定出来るだろう。

問1。 命題の例を5つ挙げて、特称のときと全称のときに真偽がどうなるかを示せ。

ここでさらに、一般の命題でも扱える形に書き直してみよう。 $Q, R$  を一つの変数を含む命題で、 $Q(x) = 「x$  は  $A$  である」、 $R(x) = 「x$  は  $B$  である」という形とする。このとき「 $A$  は  $B$  である」というのを「 $x$  が  $A$  であれば、 $x$  は  $B$  である」と言い換えてもよく、さらに「 $Q(x)$  が真ならば、 $R(x)$  は真である」と言い直せ、これを論理記号で  $x(Q(x) \implies R(x))$  と書くのである。

しかし、これだけでは、 $P = 「A$  は  $B$  である」を命題と言うわけにはいかない。 $x$  という変数がどのように振る舞うかの指定が必要で、それを指定するのが全称、特称ということである。

特称命題「ある  $A$  は  $B$  である」=「 $B$  である  $A$  が存在する」を  $\exists a(Q(a) \implies R(a))$  と書き、全称命題「すべての  $A$  は  $B$  である」を  $\forall a(Q(a) \implies R(a))$  と書く。

しかし全称か特称かを一々言うのが面倒だと思う人も多く、何も言わず「 $A$  は  $B$  である」と言えば全称命題のことで、特称命題の時だけそのことを断るという使い方が日常的には多いようである<sup>13</sup>。

集合  $M = \{a|Q(a)\}$  を考えれば、上の論理式はそれぞれ  $\exists a \in M$  ( $R(a)$ )、 $\forall a \in M(R(a))$  と書いても良い。(  $\exists$  を 存在作用素 と言い、 $\forall$  を 全称作用素 と言う。 )

さらに集合  $N = \{a|R(a)\}$  を考えれば、上の論理式は集合算で表わすことが出来る。特称命題  $\exists a \in M(R(a))$  は  $M \cap N \neq \emptyset$  を表わしており、非存在 ( $\emptyset$ ) の否定として存在 ( $\neq \emptyset$ ) を表わしている。また全称命題  $\forall a \in M(R(a))$  は 包含関係  $M \subset N$  を表わしており、「 $Q$  ならば  $R$  である ( $Q \implies R$ )」という含意を言い換えたものと言える。

以下、基本命題から複雑な命題を得ていく過程を考えよう。

<sup>13</sup> しかしこれははっきりとした取り決めになっているわけではなく、聞いている人に全称のことだと思わせておいて実は特称だったというレトリックを使う人達がいる。全称・特称の勘違いに気持ちを向けておいて、肝心の主張に疑問を感じさせないようにし受け入れさせてしまうのである。テレビで種々の討論を聴く機会が増えたが、全称・特称に気をつけて聞いているだけでも、色々なことが見えてくる。

変数を含んでいない命題「 $A$ は $B$ である」も変数を含む命題を使って仮言命題<sup>14</sup>の形に表わすことが出来たので、命題は常に変数を含んでいると考えてもよい。命題 $P(x)$ が変数 $x$ を含んでいるとは、命題 $P$ は $x$ を何か特定したとき真か偽かが確定しているということである。

集合 $M_P = \{x|P(x)\}$ は命題 $P(x)$ が真である元を集めた集合であるが、言い換えれば命題 $P$ が成り立つ範囲であるとも言える。そうすれば幾つかの命題 $P, Q, R, \dots$ に対して、対応する集合の集合算に対応する命題が考えられるだろう。

$M = M_P, N = M_Q, L = M_R$ とすると、和集合 $M \cup N$ に対しては論理和 $P \vee Q$ ( $P$ または $Q$ )が対応し、共通部分 $M \cap N$ に対しては論理積 $P \wedge Q$ ( $P$ かつ $Q$ )が対応している。含意( $P \implies Q$ ( $P$ ならば $Q$ ))も、包含関係 $M \subset N$ に対応していた。古典的な三段論法

$$(P \implies Q) \wedge (Q \implies R) \implies (P \implies R)$$

も包含関係の推移律

$$M \subset N \text{ かつ } N \subset L \text{ ならば } M \subset L$$

に対応しているのである。<sup>15</sup>

問2。正しい三段論法の例を5通り以上、誤った推論の例を5通り以上挙げよ。

補集合 $M^c$ に対応する命題は $P(x)$ の否定命題 $\neg P(x)$ であるが、これが考えだすとなかなか難しい。「 $x$ はリンゴである」の否定命題は「 $x$ はリンゴでない」である。これには問題はないようだ。しかし、「 $x$ は大きい」の否定命題となると、「 $x$ は小さい」とすべきか「 $x$ は大きくない」とすべきか、現実的には迷うところである。数学としては、命題の真偽が確定していないといけないので、「 $x$ は大きくない」に統一することにする。つまり、命題 $P(x)$ の否定命題 $\neg P(x)$ は、 $P(x)$ が真のとき偽で、偽のとき真であるような命題のこととするのである。

このように定義するのであるから、複合命題 $P(x) \vee \neg P(x)$ は常に真で、 $P(x) \wedge \neg P(x)$ は常に偽である。

当然のようなこの結論のことを排中律と言う。真と偽の間を認めないということである。しかし、排中律はすべての論理学者・数学者が認めているという訳ではない。勿論、多くの数学者は排中律の上に立って仕事をしているのであり、排中律を認めないという数学者に出会ったことはないのだけれど。

ともかく、排中律自体は証明できる性質のものではなく、論理の運用のための要請としておかれたものである。従って、排中律を認める、つまり、白でも黒でもない「灰色」を認めないという立場で論理を運用しているのである。しかし現実的にはそうでない場合に出会うことも多い訳で、数学が机上の空論と見られかねない根拠もここにあるのである。

現在では数学も灰色を認める、つまり排中律を認めない論理学も作られており、特に人間の脳に関する議論には有効なようであるが、だからと言って、その論理に従うことを主

<sup>14</sup> 「 $Q$ ならば $R$ である」という命題のこと。 $Q$ であることのなかに $R$ であることが含まれているという意味で「含意」という言葉を用いるが、変数 $x$ を意識して、仮に $x$ が $Q$ であるとすれば $x$ が $R$ であることが言えるという意味で使う。

<sup>15</sup> 真であることが確定している命題から新しく真である命題を作る方法は古典的にはこの三段論法しかない。詭弁の発達した古代ギリシャ時代には、これに似て非なる論法が横行したようで、4つの格の $(2^3)^3 = 8^3 = 256 \times 2$ 通りの三段論法に分類され、そのうち正しいものは24通りにすぎない。格は前提の各仮言命題の前後の入れ替えで得られ、他のものは全称特称の別、肯定否定の別によるものである。

張ることによって、排中律の基盤の上に建っている全理論科学を捨て去ることが出来る訳ではない。

問3。 排中律を肯定する立場と否定する立場に分かれてディベートを行え。一人の場合には、それぞれの立場の論拠を2つ以上考えた上で、自分の立場を決めよ。

問3の結果がどうであれ、本書では排中律が成り立っているものとしている。

問4。(ラッセルの集合の幽霊)すべての集合の全体がそれ自身集合だったとする。これを  $S$  と書くと、 $M = \{A \in S \mid A \notin A\} \subset S$  は集合である ( $M \in S$ ) この時、 $M$  はその存在それ自身が矛盾である、つまり集合の幽霊であることを示せ。<sup>16</sup>。

[Hint]  $M \in M \implies M \notin M, M \notin M \implies M \in M$ .

変数を含む命題  $P(x)$  は  $x$  によって真であったり偽であったりする。 $x$  が集合  $A = M_P$  に属するとき真で、属さないとき偽であった。そこで、 $A = M_P$  の元  $x$  を考えているとき、命題  $P(x)$  の真理値は T(true) であり、 $x \in A^c$  に対しては  $P(x)$  の真理値は F(false) であるということにする。

基本命題  $P, Q, R, \dots$  の真理値が分かっているとき、複合命題  $\neg P, P \vee Q, P \wedge Q, P \implies Q$  などの真理値が分かるだろうか？

それは対応する集合の集合算を見てやれば分かるのである。例えば、 $P \wedge Q$  は  $P$  と  $Q$  の真理値が共に T のときだけ T となるのである。しかし、含意  $P \implies Q$  は  $A \subset B (= M_Q)$  となるだけで真理値が分からないような気がするかもしれない。

$A \subset B$  をもう少し考えて見よう。 $A$  の元は必ず  $B$  の元であることであった<sup>17</sup>。これを言い換えると、 $A$  の元であるにも係らず  $B$  の元でないという元はない、更には  $A$  の元であって  $B^c$  の元でもあるものはないということになり、 $A \cap B^c = \emptyset$  という式で表現される。ベン図を描けばこれが  $A \subset B$  と同じことであるのはすぐに分かるだろう。補集合を取れば、 $A^c \cup B = \Omega$ <sup>18</sup> となる。 $A^c \cup B$  に対応する命題は  $\neg P \vee Q$  となり、これを含意  $P \implies Q$  の定義とすることにするのである。

$P, Q$  (つまり  $A, B$ ) の係り方次第で、( $P, Q$  がたとえ真でも偽でも) 仮言命題  $P \implies Q$  は命題として (常に) 真であることが有り得るのである。むしろ仮言命題こそが常に真でありうるのだということが言える。

例えば次のような例を考えてみる。

「明日天気なら、遠足に行く」

と学校の掲示板に告示があったとする。明日天気なら、確かに遠足に行くのであってこれは問題がない。しかし明日天気でなかったらどうなるのだろうか？雨をおして遠足に行っ

<sup>16</sup>  $S$  を集合としたから矛盾が出たのだが、そのとき  $S \in S \setminus M$  であり、普通の集合はみな  $M$  に属している。 $S$  自身が幽霊と言うのではなく、普通に扱わねばならない集合を全て集めてきたら  $M$  という矛盾を孕んだものが生まれたことに、このパラドックスの深刻さがある。排中律の副産物とも言える。

<sup>17</sup> ここ以前の、集合を扱っている節で、包含関係の意味について説明している。

<sup>18</sup> これも集合の節で議論していることだが、 $\Omega$  は宇宙 (Universe) という名前の集合である。つまり、ラッセルのパラドックスがあるため、集合全体の集合を考えることが出来ず、そのとき考察している対象すべてを含む集合を  $\Omega$  と呼び、考察の対象をこの集合の元に限るのである。もちろんこの集合を意識しないでも済む多くの場合には、省略することになっている。

ある意味では、考察する対象のすべてが集合をなすように自己規制していることになる。数学者にとっても、宇宙  $\Omega$  を特定することが一番難しいということも有り得る。

たととしても、雨だから遠足が中止になったとしても揭示の文章が間違っていたとは誰も思わないだろう。 $P =$ 「明日天気である」、 $Q =$ 「明日遠足に行く」として $P \implies Q$ であるという揭示そのものは、無責任と言われるかもしれないが、間違っただけではなかったことになる。明日天気であっても遠足に行かないということだけではないと言っているのである<sup>19</sup>。

仮言命題 $P \implies Q$ の命題の位置を逆にした命題 $Q \implies P$ を逆といい、各命題を否定にしたもの $\neg P \implies \neg Q$ を裏と言い、否定にして順序を逆にしたもの $\neg Q \implies \neg P$ を対偶と言う。

これらに対しても真理値がどうなるか、真理表<sup>†</sup>を挙げておこう。

$P$	$Q$	$\neg P$	$\neg Q$	$P \vee Q$	$P \wedge Q$	$P \implies Q$	$Q \implies P$	$\neg P \implies \neg Q$	$\neg Q \implies \neg P$
$T$	$T$	$F$	$F$	$T$	$T$	$T$	$T$	$T$	$T$
$T$	$F$	$F$	$T$	$T$	$F$	$F$	$T$	$T$	$F$
$F$	$T$	$T$	$F$	$T$	$F$	$T$	$F$	$F$	$T$
$F$	$F$	$T$	$T$	$F$	$F$	$T$	$T$	$T$	$T$

問題5。 i)\*) 上の真理表で、各命題に対応する集合を求め、集合算における結果と表の値が一致することを示せ。

ii) 表の各値を実現するような命題の例を作れ。

基本命題を $\forall, \exists, \neg, \vee, \wedge$ だけで結合した複合命題だけを考えることにする<sup>20</sup>。

真理表を見ると対偶の真理値と元の含意の真理値は一致しており、このことを「対偶は真」と言っているのである。

含意 $P \implies Q$ をその定義 $\neg P \vee Q$ で表すのと同じ様に対偶 $\neg Q \implies \neg P$ を書き換えれば、 $\neg(\neg Q) \vee \neg P = Q \vee \neg P = \neg P \vee Q$ であって、元の含意と全く同じ命題であることが分かる。

含意についてもう少し注意しておこう。 $P =$ 「 $Q \implies R$ 」とし、 $Q$ が真理値として $F$ しか取らないなら、つまり $Q(x)$ が真であるような $x$ が存在しなかったならどうなるのだろうか？真理表によれば $R$ の真理値がどうであれ、含意 $P$ は真であるということになる。このことを仮言命題「 $Q \implies R$ 」は、無内容的に成り立つと言うのである。

対応する集合で考えて見よう。 $A = M_Q, B = M_R$ とおくとき、 $A \subset B$ となるわけだが、 $Q$ が $F$ しか真理値を取らないということは $A = \emptyset$ ということであり、どんな集合 $B$ に対しても $\emptyset \subset B$ が成り立つということである。

このように論理だけで分かりにくいときは、対応する集合の言葉で言い換えると分かりやすくなることがある。

まだ言うべきこともあるが、これでも十分長くなった。パズルを一つ挙げて、この節を終えることにしよう。

問題6。 昔ある男が病気の母のために、万病に効く靈芝を取りに山に行った。山には

<sup>19</sup> 雨が降るのを天気でないこととしている。降ったり止んだりしていたらどうなるのという疑問はもっともではあるが、この際問題にしていることではない。天気であるということの判定が微妙で命題とは言いがたいという反論には抵抗する気も起らない。不満な読者はもっとはっきりした例を自分で作って欲しい。例えば、「ソクラテスが日本人なら、ジンギス汗は源義経だ」というのは如何でしょう。

<sup>20</sup> 複合命題についてもう少し述べる必要がある。例えば、 $\neg(\neg P) = P, P \vee Q = Q \vee P, \neg(P \vee Q) = \neg P \wedge \neg Q$ などの規則を与えるなど。しかし、本書の程度ではこれ位にして置いたほうがよいだろう。

双子の子鬼がいて、靈芝を守っていた。何が靈芝かを知っているのは子鬼だけである。靈芝に良く似た毒キノコもあって、靈芝の乱獲を防いでいる。兄の子鬼は正直もので嘘をつかないが、弟はいたずらもので嘘しか言わない。しかも、人間の言葉を話すのが苦手で、「うん」か「いや」しか言えないし、一言喋ると人前から隠れてしまう。

男はやっと一人の子鬼を見つけ、靈芝らしいキノコも2種類見つけた。男はどちらのキノコが靈芝かを、たった一つの質問をして、子鬼から訊き出した。男の母親は救われた。

さて、男はどんな質問をしたのだろうか？

[Hint] 例えば、「お前は正直ものか？」と訊いても、返ってくる答えは「うん」に決まっ  
ていて、兄弟どちらか分からない。

\*\*\*\*\*

[数学教育史コラム]<sup>†</sup> 真理表はどこへ行った

(「小学校教師の」と銘打ったので、各節に関する教育史のコラムを入れるつもりであるが、人に頼むのか自分たちでやるのか決心がついていない。) æ

### 3 アミダくじと組み紐の群 (美杉セミナー'94)

1994年6月25日に名城大学の総合講座の一つとして行った講演を、1994年度の高校生セミナーのためにアミダくじの図を少し丁寧に書き直して、1995年3月11日に行ったものの記録を、紙上でも読みやすいように手を入れたものである。

#### 3.1 対称群とアミダ群

高校までの数学は、図形、数、関数、確率を主な対象としているが、集合、論理、組み合わせ論、また2行2列の行列  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  も取り扱っている。

大学に入れば、2より大きな  $n$  に対する  $n$  行  $n$  列の行列も考えることになるが、そのとき行列式というものが重要になる。行列式は2行2列のときは簡単で  $ad - bc$  に過ぎないが、一般の  $n$  になると定義することさえ難しいものになる。その行列式の定義に  $n$  次対称群  $S_n$  というものが出てくる。 $n$  文字の集合の置換の全体である。

$n$  文字の集合は  $I_n = \{1, 2, \dots, n\}$  という数の集合と同じだと考えることが出来る。置換とはその  $(1, 2, \dots, n)$  番目にどんな数か来るかを指定することにあたるのだから、 $n$  文字の順列を与えることと同じになる。そこで、順列を並び変える手続きを演算として群と考えたものであった。置換の総数は  $n!$  個である。

意味のある群のもっとも簡単な例であって、ガロアが群を導入したとき以来人類にとって馴染みの深い群である。

しかし、これは分かりやすいとは言えないものである。

集合としては、 $S_n = \{\sigma : I_n = \{1, 2, \dots, n\} \rightarrow I_n; \text{全単射} = 1 \text{ 対 } 1 \text{ 対応}\}$  と定義してしまえば良いし、写像の合成を群演算(積)と考えれば良い。それだけの状況で、厳密な議論が進行するのだが、高校レベルよりは少し高度な数学的概念や思考法が必要となる。

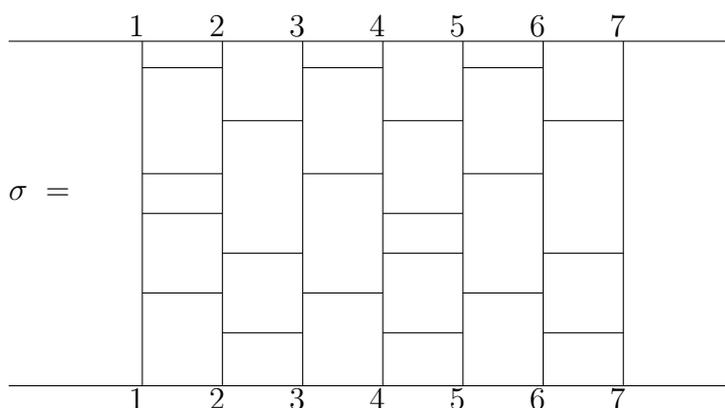
実は、アミダくじを使うことによって、この群の性質を視覚的に見ることに出来る。この話では、アミダくじを少し厳密に考え、演算を定義し、構造を調べてみることにしたい。

対称群との対応を考えるために、まず  $n$  文字の置換をどう表すかを書いておこう。 $n = 7$  のとき、例えば置換は  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 5 & 4 & 1 & 7 \end{pmatrix}$  と表される。これは上の列の数  $i$  に対応する数  $j = \sigma(i)$  をその下に書いて表したものである。1は2に、2は3に、3は6に、4は5に、…… などということになる。

さて、 $n$  本のアミダくじ全体を考え、それに群の構造を入れるということを考えよう。

まず2本の水平線の間を  $n$  本の垂直な線分で結ぶ。等間隔である必要はないが、そうしない理由もないので、等間隔に引くことにする。各垂線の上下の端点に、垂線が左から数えて何番目かを表す数を書いておく。隣り合った垂線の間を水平な線分(橋と呼んでおく)で結びたいだけ(0本でも良い)結ぶ。この図形を「アミダくじ」と呼んでいる。

$n = 7$  での例を一つ挙げておこう。



くじとして使うためには、何が何に当たるのかを指定しなければならない。上の水平線の番号を選んで ( $i$  とする)、垂線を下りて行き、橋に出会ったら、必ず橋を渡ることにして、下の水平線まで進み、そこにある番号 ( $j$  とする) をみる<sup>21</sup>。このときアミダくじ  $\sigma$  は  $i$  を  $j = \sigma(i)$  に対応させたということにする。こうして得られた対応は、 $I_7$  の置換になっており、上に挙げた例の  $\sigma$  と同じである。アミダくじの目的からいえば、この対応表さえあれば良いことになる。

そこで、同じ対応 (置換) を与えるアミダくじは同値であると言ってもいいし、更に一歩進んで同じものであると思ってもいい。そこで、アミダくじとそれが与える置換とを同じ記号 (この場合は  $\sigma$ ) を使って表すことも多い。

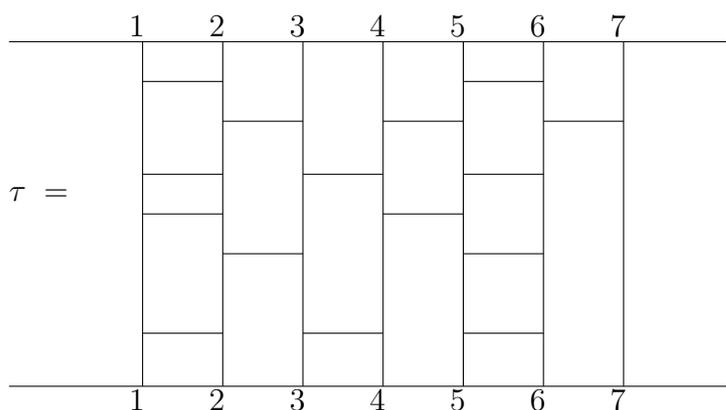
同値なくじを同じものだと思ったものを元とする集合を  $\mathcal{A}_n$  と書く。つまり、くじを置換だと考えることにあたっているので、 $\mathcal{A}_n \subset S_n$  と考えていることになる。また、後で示すように群になるので、 $n$  次のアミダ群 と呼ぶことにしよう。

例えば、パーティなどで  $n$  人の人が  $n$  個の品物を選ぶというとき、人と品物に番号を付けておけば、アミダくじが使われることになる。例えば、上のアミダくじでは、1 番の人は 2 番の品物を、2 番の人は 3 番の品物を、3 番の人は 6 番の品物を、…… などということになる。

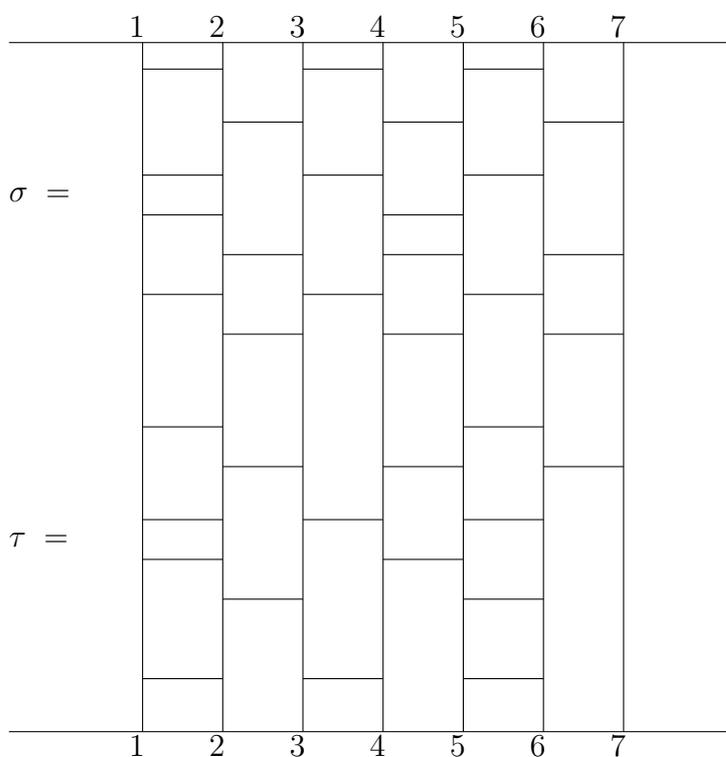
このとき、1 回のアミダくじでは不満だという人がいたらどうしたら良いだろう。別のアミダくじを使って、2 回やることにすると、どうすることになるだろうか。1 度目のくじ  $\sigma$  で 2 度目のくじ  $\tau$  の上の水平線の番号を決めることにしたらどうだろうか。

この手続きを図形としてのアミダくじでは、次のように考えれば良いだろう。まず  $\sigma$  と  $\tau$  を描き、 $\sigma$  の下の水平線と  $\tau$  の上の水平線を同じ番号が重なるように重ね合わせ、その後、この重なった水平線を消去する。例えば、 $\tau$  を

<sup>21</sup> この進み方を確定するために、垂線上の点は二つ以上の橋の端点になってはいけないという制限を課しておく。



とすると、



というアミダくじを考えることになる。これを  $\sigma$  と  $\tau$  との積  $\tau \cdot \sigma$  と書くことにする。この順序は、くじを対応と考えた時の合成に当たっている。つまり、 $\tau \cdot \sigma(i) = \tau \circ \sigma(i) = \tau(\sigma(i))$  である。

置換だと考えると

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 4 & 6 & 7 & 1 & 3 \end{pmatrix}$$

であって、積  $\tau \cdot \sigma$  は

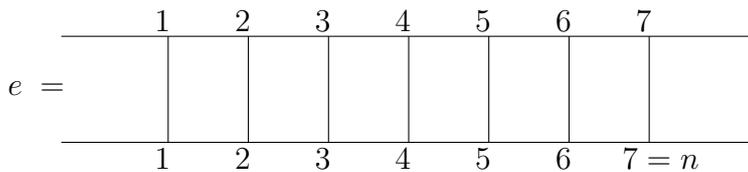
$$\tau \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 4 & 6 & 7 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 5 & 4 & 1 & 7 \end{pmatrix}$$

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

となっている。この積で集合  $A_n$  が群になることが分かる。群であることは、3つの性質（結合法則、単位元の存在、逆元の存在）を確かめないといけない。

しかしそれは簡単に確かめられる。結合法則は積がくじを繋いで行くことから考えれば明らかだし、単位元  $e$  は橋の一つもないアミダくじで、任意の元  $\sigma$  の逆元  $\sigma^{-1}$  は上下の水平線を交換するように折り返したものにすれば良い。図を描きながら考えれば難しくないだろう。

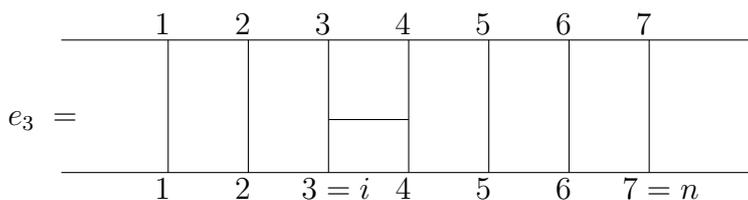
橋が一つもないのも立派な対応で、



これが単位元  $e$  である。置換で書けば、 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$  であって、どの順番も変えないものである。

$i$  番目の人が  $i$  番目の品物をとるのは面白味がないと思うかもしれないが、これが基本である。 $i$  番目の品物は  $i$  番目の人が持って来たものということであれば、自分の持って来た品物を持って帰ることに当たっている。また一般に  $\sigma(i) = j$  は、 $i$  番目の人が  $j$  番目の人にプレゼントしたことに当たっており、逆の  $\sigma^{-1}$  は自分にプレゼントしてくれたことになる人物は？という対応になっている。

さて、積が上のように定義されれば、すべてのアミダくじは、橋が1つだけのアミダくじを橋の数だけ次々と掛けたものになる。 $i$  番目の垂線と  $i+1$  番目の垂線とを一つの橋で結んだだけのアミダくじを  $e_i$  と書けば、



という図になる。置換で書けば  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 5 & 6 & 7 \end{pmatrix} = (3,4)$  と書ける。これは3と4だけを動かし、それを交換するので3と4の互換と言い、 $(3,4)$  とだけ表すことがある。

すべてのアミダくじ  $\sigma$  は  $e_i$  達の積で表されることになる<sup>22</sup>。このことを、アミダ群  $A_n$  は  $n-1$  個の元  $e_i (1 \leq i \leq n-1)$  で生成されるという。

最初に挙げた例の  $\sigma$  は  $e_2 e_4 e_6 e_1 e_3 e_5 e_2 e_4 e_6 e_1 e_4 e_1 e_3 e_5 e_2 e_4 e_6 e_1 e_3 e_5$  と表される。図で見ると積は上から下へ、 $e_i$  の積で表わす時は右から左への順に作用していると思っている。

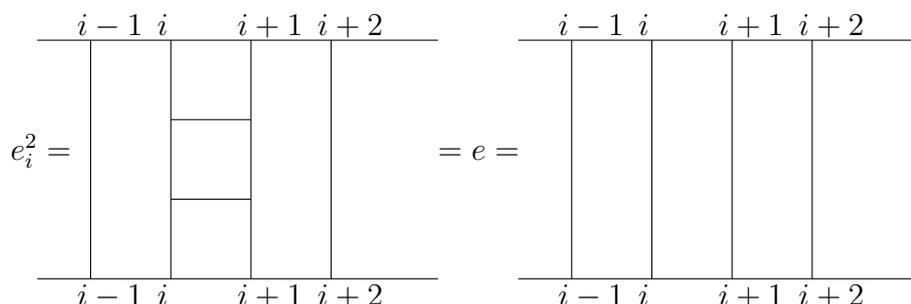
<sup>22</sup>  $i$  番目の垂線と  $i+1$  番目の垂線に橋を1本架けることが、 $e_i$  を掛けることに当たっている。

ところで、あらゆる  $e_i (1 \leq i \leq n-1)$  の語 (ワード) <sup>23</sup> が、異なる対応を与えている訳ではない。 $e_i (1 \leq i \leq n-1)$  の生成する自由群  $F_{n-1} = \{e_{i_k} \cdots e_{i_2} e_{i_1}; 0 \leq k, 1 \leq i_j \leq n-1 (1 \leq j \leq k)\}$  がワードの全体<sup>24</sup> だが、この無限群  $F_{n-1}$  を  $I_n$  の置換として同じものを同じと見るという同値関係で割ったものが  $\mathcal{A}_n$  である。

生成元は  $\{e_i (1 \leq i \leq n-1)\}$  より減らすことは出来そうもないが、関係式の方は出来るだけ減らしたい。

自明な関係を考えてみる。まず、(橋を行って戻るだけだから)

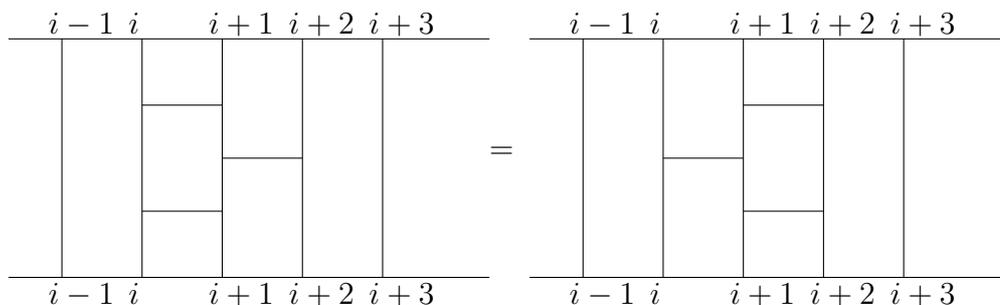
$$(1) \quad e_i^2 = e$$



が成り立つことは、明らかであろう。 $e_i^{-1} = e_i$  である。

また

$$(2) \quad e_i e_{i+1} e_i = e_{i+1} e_i e_{i+1}$$



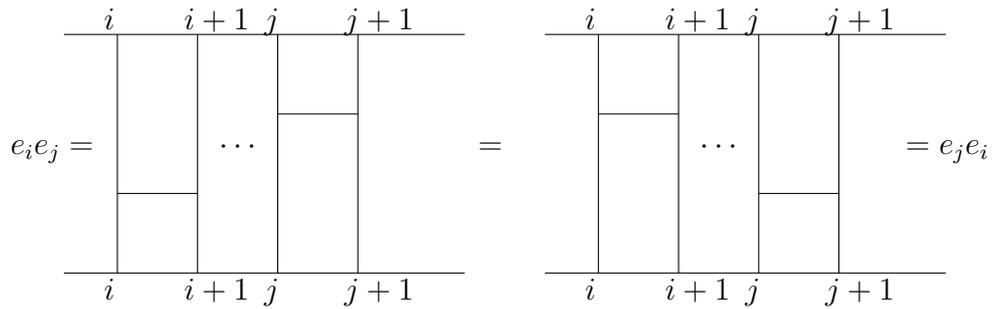
が共に互換  $(i, i+2)$  を表していることも容易に分かる。 $i$  と  $i+2$  は同じ様に階段を下りるだけだが、真ん中の  $i+1$  は一旦隣に行き行って戻って来る訳で、隣というのが両側にあるから二通りの表現を持つということである。

関係式はもう一種類ある。

$$(3) \quad e_i e_j = e_j e_i \quad (|i - j| \geq 2)$$

<sup>23</sup> 好きな順序で好きなだけ掛けたもの

<sup>24</sup> これが図形としてのアミダくじの全体に当たる



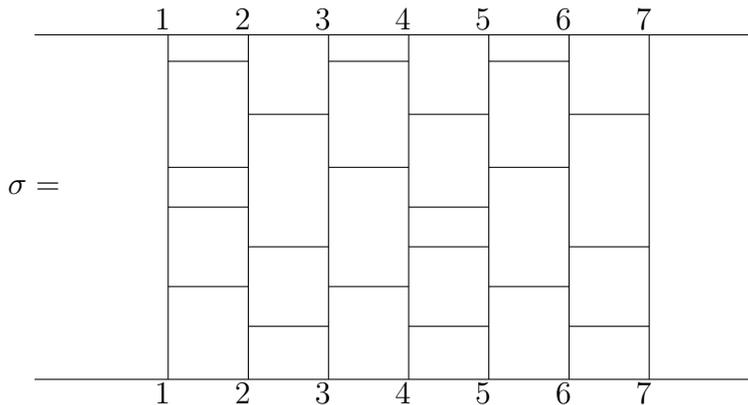
$e_i$  と  $e_j$  は離れた垂線同士を結ぶ橋なので、他の橋の端点にぶつからない限り、橋の位置をどのように上下させても良いということである。

この3種類の関係式が基本関係式になることと、 $\mathcal{A}_n = \mathcal{S}_n$ 、つまり  $e_i$  の積ですべての順列が得られることが、この話のメインテーマの一つである。

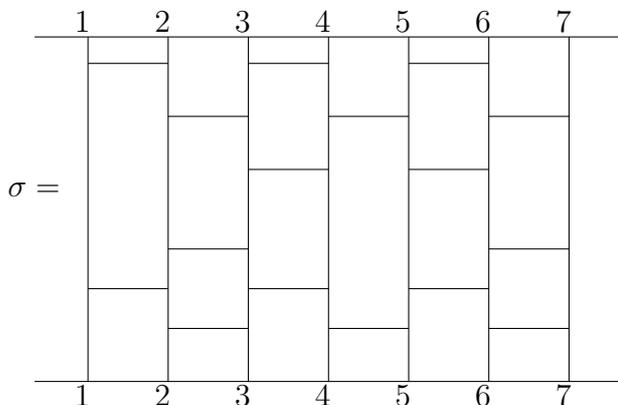
例でやって見よう。最初与えたアミダくじは

$$\sigma = e_2 e_4 e_6 e_1 e_3 e_5 e_2 e_4 e_6 e_1 e_4 e_1 e_3 e_5 e_2 e_4 e_6 e_1 e_3 e_5$$

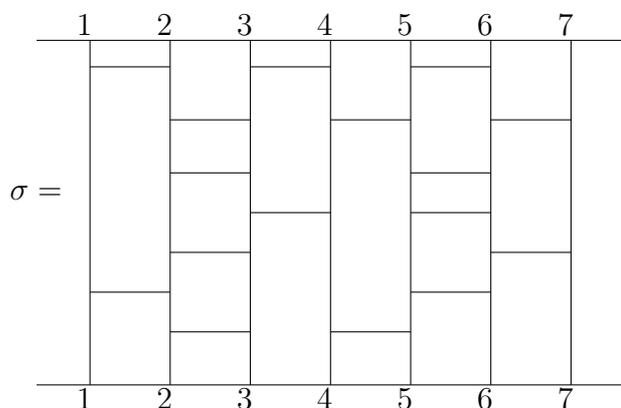
であった。もう一度描いて見よう。



(3) と (1) の  $e_1^2 = e$ ,  $e_4^2 = e$  から  $\sigma = e_2 e_4 e_6 e_1 e_3 e_5 e_2 e_6 e_3 e_5 e_2 e_4 e_6 e_1 e_3 e_5$  となることを、図で書けば

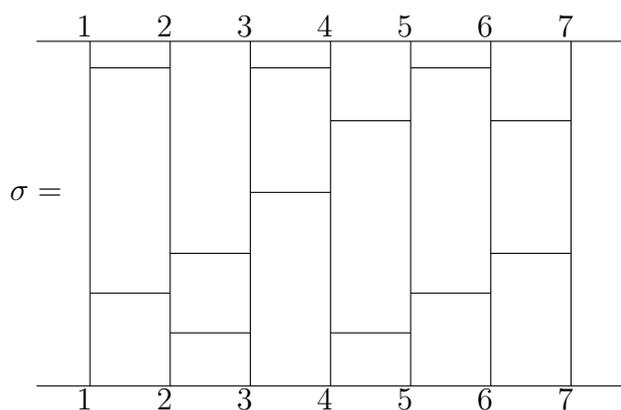


となり、(3) と (2) の  $e_3e_2e_3 = e_2e_3e_2, e_6e_5e_6 = e_5e_6e_5$  を使えば、 $\sigma = e_2e_4e_5e_1e_2e_6e_3e_5e_2e_5e_2e_4e_6e_1e_3e_5$  となる。図に書けば

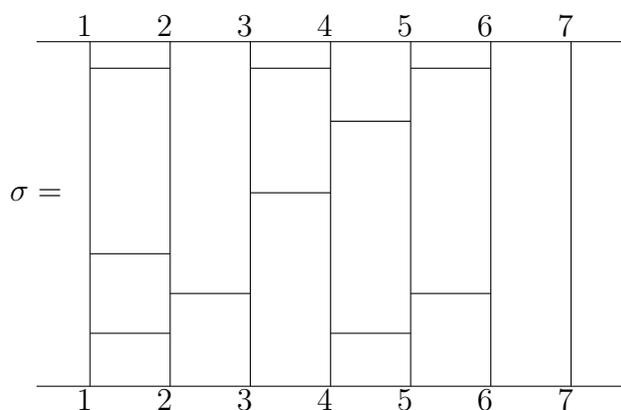


となる。さらに、(3) と (1) の  $e_2^2 = e, e_5^2 = e$  から

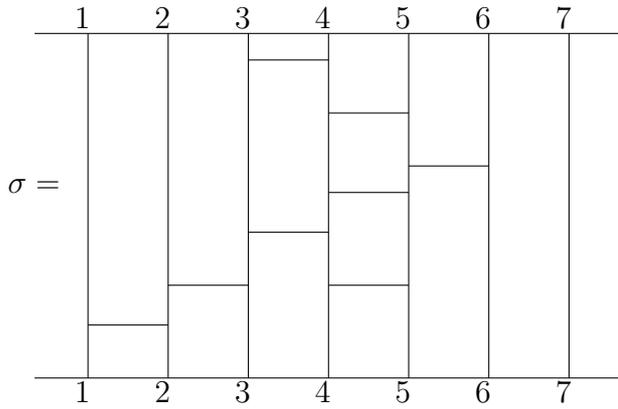
$$\sigma = e_2e_4e_5e_1e_2e_6e_3e_4e_6e_1e_3e_5$$



となり、(3) と (1) の  $e_6^2 = e$  と (2) の  $e_2e_1e_2 = e_1e_2e_1$  を使えば、 $\sigma = e_1e_4e_5e_2e_1e_3e_4e_1e_3e_5$

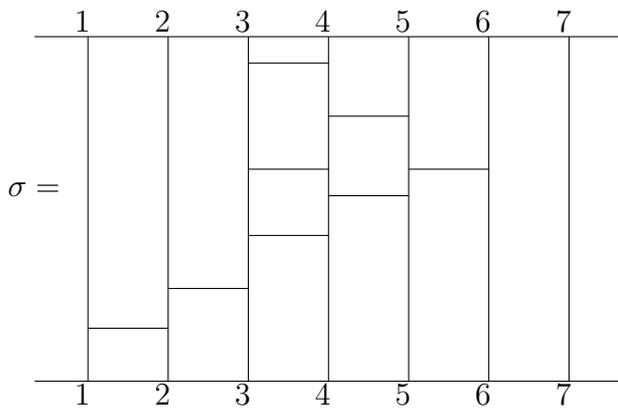


となる。さらに、(3) と (1) の  $e_1^2 = e$  と (2) の  $e_5e_4e_5 = e_4e_5e_4$  を使えば、 $\sigma = e_1e_4e_2e_3e_4e_5e_4e_3$



となる。最後に、(3) と (2) の  $e_4e_3e_4 = e_3e_4e_3$  を使えば、

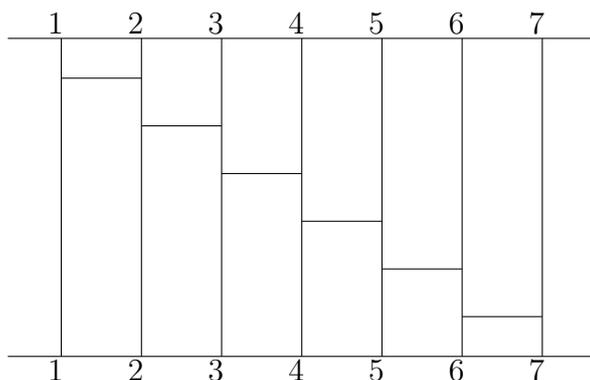
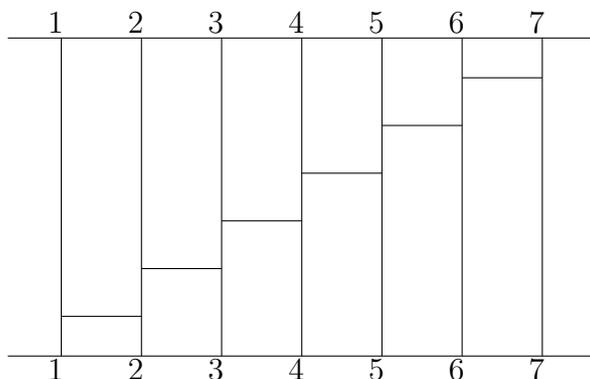
$$\sigma = e_1e_2e_3e_4e_5e_3e_4e_3 = f_1^{(6)} f_3^{(5)} f_3^{(4)}$$



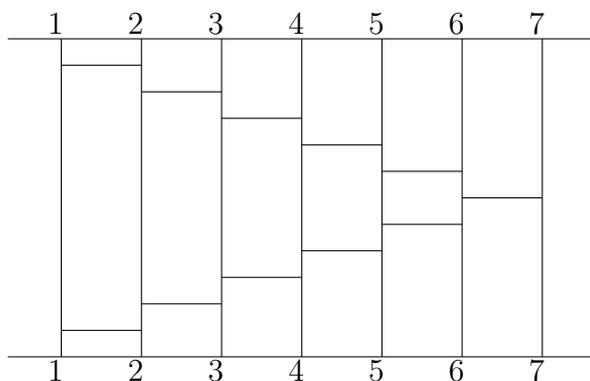
と、簡便な表示が得られる。ここで、 $f_i^{(n)}$  は次節で定義する、左下がりの階段を表す標準的な元で、一般の元  $\sigma$  の標準表示に使うものである。æ

### 3.2 アミダ群の特別な元

(3) によって多くの  $e_i$  (橋) は互いにすり抜けるが、隣り合う橋は引っ掛かって抜けられず、特別な形のアミダが重要になる。例えば、次のような階段状のアミダはこれ以上簡明にならない。

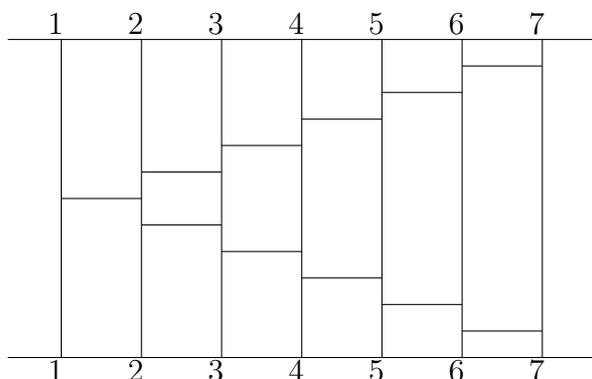


左下がりの階段  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$  は前から後ろへの巡回置換 (1234567) で、右下がりの階段  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$  は後ろから前への巡回置換 (7654321) になる。往復の階段を組み合わせると、



を考えると、置換としては  $(123456)(7654321) = (17)$  となり、両端の 1 と 7 を交換する互換になる。

階段の順は右下がりの後でも前にしても同じになる筈で、逆の順序にした



というアミダくじは置換とすると  $(765432)(1234567) = (17)$  となる。

階段のうちでも、右端が  $n$  であるものは特に重要で、左下がりの方に名前を付けておこう。

各  $1 \leq i \leq n-1$  に対して元  $f_i = e_i e_{i+1} \cdots e_{n-1} \in F_{n-1}$  を考え、 $f_n = e$  とおく。帰納的に、

$$f_i = \begin{cases} e & (i = n) \\ e_i f_{i+1} & (1 \leq i \leq n-1) \end{cases}$$

としても良い。 $n$  本のアミダくじ ( $F_{n-1}$  の元) と考えていることを強調する時は  $f_i$  を  $f_i^{(n)}$  と書くことにする。すると、 $f_i^{(n)} = f_i^{(n-1)} e_{n-1}$  となっていることに注意しておこう。

ここで、 $\mathcal{A}_{n-1}$  は自然に  $\mathcal{A}_n$  の中に入っていると思っている。つまり、 $\mathcal{A}_{n-1}$  の元  $\sigma$  に対し、 $n$  本目の垂線をその右に付け加えた  $\mathcal{A}_n$  の元を考えて、それを改めて  $\sigma$  と書くことにする。このような元  $\sigma$  に対しては  $\sigma(n) = n$  である。この関係により次々と

$$\{e\} = \mathcal{A}_1 \subset \mathcal{A}_2 \subset \mathcal{A}_3 \subset \cdots \subset \mathcal{A}_{n-1} \subset \mathcal{A}_n$$

のように、中に中に入っていると思っているのである。

また関係式 (1) だけから、 $f_i^{-1} = e_{n-1} \cdots e_{i+1} e_i$  (右下がりの階段) であることは分かる。

$\mathcal{A}_n$  の元としては、 $i < j$  のとき、 $f_i^{(j)} = (i, i+1, \dots, j-1, j)$  であり、 $(f_i^{(j)})^{-1} = (j, j-1, \dots, i+1, i)$  である。それゆえ、上の互換は任意の二つに対しても同じ往復の階段で表現され、 $(i, j) = (f_i^{(j-1)})^{-1} f_i^{(j)} = f_i^{(j-1)} (f_i^{(j)})^{-1}$  となっている。こうして、互換  $(i, j)$  は  $2(j-i)-1$  という奇数個の  $e_k$  の積で表わされている。

この特別な階段を用いて、 $\mathcal{A}_n = \mathcal{S}_n$  であることを示しておこう。

[証明] まず、 $\mathcal{A}_n \subset \mathcal{S}_n$  であることから、集合としての元の個数が  $\#\mathcal{A}_n \leq \#\mathcal{S}_n = n!$  であることに注意しておく。 $n$  が小さいうちは簡単で、 $\mathcal{A}_1 = \{e\} = \mathcal{S}_1$ ,  $\mathcal{A}_2 = \{e, e_1\} = \mathcal{S}_2$  となっている。実際、

$$e_1^k = \begin{cases} e & (k: \text{偶数}) \\ e_1 & (k: \text{奇数}) \end{cases}$$

である。

各  $n$  に対して、 $\cup_{i=1}^n f_i \mathcal{A}_{n-1} \subset \mathcal{A}_n$  は互いに交わらない和である。

何故なら、 $\sigma \in \mathcal{S}_{n-1}$  に対して、

$$f_i \sigma(j) = \begin{cases} \sigma(j) & (\sigma(j) < i) \\ \sigma(j) + 1 & (i \leq \sigma(j) < n) \\ i & (j = n) \end{cases}$$

となる。 $\sigma$  を作用させた後で、 $n$  を  $i$  へ持って行き、 $i$  以降を一つ後ろにずらすということを表している。

従って、 $f_i \sigma = f_k \tau$  ( $\sigma, \tau \in \mathcal{S}_{n-1}$ ) とすれば、 $i = f_i \sigma(n) = f_k \tau(n) = k$  だから、 $i = k$  であって、両辺に  $f_i^{-1}$  を施せば、 $\sigma = \tau$  となる。

[証明終]

$f_i \mathcal{A}_{n-1}$  が互いに交わらないから、

$$\#\mathcal{A}_n \geq n \#\mathcal{A}_{n-1}$$

となり、次々とみれば

$$\#\mathcal{A}_n \geq n \#\mathcal{A}_{n-1} \geq n(n-1) \#\mathcal{A}_{n-2} \geq \cdots \geq n(n-1) \cdots 3 \#\mathcal{A}_2 = n!$$

となるから、逆向きの不等式を合わせて  $\#\mathcal{A}_n = n!$  となる。元の個数が等しい部分集合は全体に一致することから、 $\mathcal{A}_n = \mathcal{S}_n$  であることが分かる。

[証明終]

ところで、 $\mathcal{A}_n$  の元  $\sigma$  は  $e_i$  達の積になっているのだが、それがどんなものになるのかわからない。例えば、 $\sigma(n) = n$  だからといって、 $e_{n-1}$  を含んでない  $\sigma$  の表示が有りうるかどうかさえ明らかではない。出来れば標準的な方法で、一通りに書けると、分かり易いと思う。これを実現するのが標準形の問題だが、まず関係式は (1)~(3) 以外のものが不要であることを示すことにしよう。

このことを確かめるために、 $e_i$  達のワードの全体である自由群  $F_{n-1}$  を (1)~(3) の関係式だけで割った群に  $\mathcal{B}_n$  という名前をつけ、この群がアミダ群と一致することを示すことにする。

アミダ群  $\mathcal{A}_n$  では、(1)~(3) の関係式が成り立つのだから、 $\mathcal{A}_n$  の元として同じものは  $\mathcal{B}_n$  の元として同じである。つまり、 $\mathcal{A}_n$  には、それ以外の関係式も成り立っているかもしれないから<sup>25</sup>、 $n! = \#\mathcal{A}_n \leq \#\mathcal{B}_n$  ということになる。

したがって、 $\#\mathcal{B}_n \leq n!$  が言えれば、 $\#\mathcal{A}_n = n!$  が分かっているので、 $\#\mathcal{B}_n = n!$  が分かり、従って  $\mathcal{B}_n = \mathcal{A}_n$  であることが分かる。

以下、 $\#\mathcal{B}_n \leq n!$  を示すことにする。

任意の元  $\sigma \in \mathcal{B}_n$  は  $\mathcal{B}_{n-1}$  の元であるか、 $\sigma = \omega e_{n-1} \tau$ ;  $\omega, \tau \in \mathcal{B}_{n-1}$  の形に表わすことが出来る。

このときもっと強いことが言えて、任意の元  $\sigma \in \mathcal{B}_n$  は  $\sigma = f_i \tau$ ;  $\tau \in \mathcal{B}_{n-1}, 1 \leq i \leq n$  の形に表わすことが出来る。 $f_i \in \mathcal{B}_n \setminus \mathcal{B}_{n-1} (1 \leq i \leq n-1)$  に注意する。

<sup>25</sup> 群論の言葉で言えば、 $\mathcal{A}_n$  が  $\mathcal{B}_n$  の商群であるということ

これは、基本関係式を使ってうまく並べ直せば、 $e_{n-1}$  は高々一つであるように出来るということである。

[証明]  $\tau \in \mathcal{B}_{n-1}$  を取る時、

$$\begin{aligned} k > i \text{ に対して} \quad e_k f_i \tau &= f_i e_{k-1} \tau \\ e_i f_i \tau &= f_{i+1} \tau \\ e_{i-1} f_i \tau &= f_{i-1} \tau \\ k < i - 1 \text{ に対して} \quad e_k f_i \tau &= f_i e_k \tau \end{aligned}$$

という関係式が得られる。

図だけの操作でもすぐ確かめられるが、紙数を取りすぎるので、ここでは式だけで証明して見よう。

$k > i$  に対し

$$\begin{aligned} e_k f_i \tau &= e_k e_i \cdots e_{k-2} e_{k-1} e_k f_{k+1} \tau = e_i \cdots e_{k-2} e_k e_{k-1} e_k f_{k+1} \tau \\ &= e_i \cdots e_{k-2} e_{k-1} e_k e_{k-1} f_{k+1} \tau = e_i \cdots e_{k-2} e_{k-1} e_k f_{k+1} e_{k-1} \tau \\ &= f_i e_{k-1} \tau \end{aligned}$$

$$e_i f_i \tau = e_i e_i f_{i+1} \tau = e f_{i+1} \tau = f_{i+1} \tau$$

後は  $f_i$  の定義と (3) とから明らか。

[証明終]

任意の元  $\sigma = e_{i_k} \cdots e_{i_2} e_{i_1} \in \mathcal{B}_n$  に対して、 $\sigma_j = e_{i_j} \cdots e_{i_2} e_{i_1} (1 \leq j \leq k)$  がある  $i$  に対して  $f_i \mathcal{B}_{n-1}$  の元であることを  $j$  に関する帰納法で証明することが出来る。

実際、 $j = 0$  のとき、 $\sigma_0 = e = f_n e$  と始めても良いし、 $j = 1$  のとき、 $\sigma_1 = f_n e_{i_1} (i_1 < n - 1)$  または  $= f_{n-1} e (i_1 = n - 1)$  と始めても良い。

帰納法の、 $j$  を大きくしていく、各段階は上の関係式からすぐに従う。

[証明終]

このことから、 $\#\mathcal{B}_n \leq n!$  を示すことができる。

最初に、 $f_i \sigma = \tau (\sigma, \tau \in \mathcal{B}_{n-1})$  であれば、 $i = n$  すなわち、 $f_i = f_n = e, \sigma = \tau$  であることを示そう。

実際、 $i \leq n - 1$  なら、 $f_i \sigma = f_i^{(n-1)} e_{n-1} \sigma = \tau$  だから、 $e_{n-1} = (f_i^{(n-1)})^{-1} \tau \sigma^{-1} \in \mathcal{B}_n$  となって矛盾。

元に戻って、 $i < j$  のとき、 $f_j^{-1} f_i = f_i f_{j-1}^{(n-1)}$  であることに注意する。

それゆえ  $f_i \sigma = f_j \tau, (\sigma, \tau \in \mathcal{B}_{n-1})$  だったとすれば、 $i = j, \sigma = \tau$  となる。

このことから、 $\mathcal{B}_n = \cup_{i=1}^n \mathcal{B}_{n-1}$  は互いに交わらない集合の和であり、 $\mathcal{B}_1 = \{e\} = \mathcal{A}_1$  であることから帰納的に

$$\#\mathcal{B}_n \leq n \#\mathcal{B}_{n-1} \leq \cdots \leq n \times (n-1) \times \cdots \times 2 \times \#\mathcal{B}_1 = n!$$

であることが分かる。

[証明終]

こうして、 $\mathcal{B}_n = \mathcal{A}_n = \mathcal{S}_n$  であることが分かったことになる。このことを対称群  $\mathcal{S}_n$  の性質としてまとめて言うことが出来る。

対称群  $\mathcal{S}_n$  は生成系  $\{e_i; 1 \leq i \leq n-1\}$  を持ち、(1)-(3) を基本関係式に持つ。

さて、今までに示したことから、対称群の元についていくつか分かることがある。

任意の元  $\sigma \in \mathcal{S}_n$  を  $e_i$  達の積で表わす時必要な  $e_i$  の個数の偶奇は定まっている。

何故なら、 $e_i$  の個数を変える関係式は (1) しかなく、そのさい常に 2 個ずつ減らすから。

[証明終]

任意の元  $\sigma \in \mathcal{S}_n$  を  $e_i$  達の積で表わすとき、左下がりの階段  $f_i^{(k)}$  (つまり巡回置換) の組み合わせで表す次のような標準形が有る。

$$\sigma = f_{i_n}^{(n)} f_{i_{n-1}}^{(n-1)} \cdots f_{i_2}^{(2)} \quad (1 \leq i_j \leq j)$$

実際、 $\sigma$  は、ある  $i$  に対して  $f_i^{(n)} \mathcal{S}_{n-1}$  に属するから、次々と

$$\begin{aligned} \sigma &= f_{i_n}^{(n)} \sigma_{n-1} && (\sigma_{n-1} \in \mathcal{S}_{n-1}) \\ &= f_{i_n}^{(n)} f_{i_{n-1}}^{(n-1)} \sigma_{n-2} && (\sigma_{n-2} \in \mathcal{S}_{n-2}) \\ &\cdots \cdots \cdots \\ &= f_{i_n}^{(n)} f_{i_{n-1}}^{(n-1)} \cdots f_{i_3}^{(3)} \sigma_2 && (\sigma_2 \in \mathcal{S}_2) \\ &= f_{i_n}^{(n)} f_{i_{n-1}}^{(n-1)} \cdots f_{i_2}^{(2)} \end{aligned}$$

であることが示される。

[証明終]

これからまた、 $\#\mathcal{S}_n = n!$  の別証明が得られる。

つまり、この標準形は表示が異なれば違う元を表していることも分かっているので、表示の数が元の数である。異なる表示の数が  $n!$  であることは見れば分かる、というわけである。

æ

## 4 終わりに

今年もまた、TOSM 事業のことや高校生への講演要旨を書かせていただくことになりました。書きたいことを書きたいだけ書いて良いという寛大さに感謝しています。

取り扱いが面倒にみえたり、少し難しくし過ぎているかもしれませんが、それなりに納得のいく答え方をしようとしたため、こうなってしまったのです。楽しんでやろうという気持ちを持って見ていただければ、面白いと思っていただける筈だと思っています。というか、こちらとしては面白いと思って書いてはいるのですが、気分が伝わっているかどうか、心配しています。

また今回は、4本ハノイの問題にしる、背理法の扱いの問題にしる、決然とした主張をしにくい問題がポストに入って、どこまで書くかの決断がなかなかつかず、書き始めるのを躊躇してもいました。

おかげで書き始めてから時間が足らなくなり、講演記録の方の推敲の時間がほとんどとれなくて、申し訳なく思っております。対称群や組み紐群の意味や重要性についても本当はもう少し述べたかったし、証明したことの内容についてもその意味や必然性について述べるつもりでしたが、時間がとれませんでした。締め切りに追われてゆっくりタイトルを考えている暇もなく、タイトルと中身に差があるというご非難も今回は特に甘んじてうけることにします。

来年は弁解せずに済むようにしたいと思っております。原稿の締め切りを何度も待って待って待って頂きましたのに、これが本当の締め切りと20分後に原稿を取りに来られる楠井先生の顔が浮かんできます。あの笑顔が今は何故か、鬼のように感じられます。原稿を渡してしまえば、また、素直に笑顔を感じられると思います。

## 参考文献

- [1] 蟹江幸博 「幾何的直観と対称性」プレプリント
- [2] 蟹江幸博 「数について(美杉セミナー '91)」'92年度数学研究会誌36号、三重県高等数学教育研究会(1992),3-41.
- [3] 蟹江幸博 「TOSM ポスト」'93年度数学研究会誌37号、三重県高等数学教育研究会(1993),2-44.
- [4] 蟹江幸博 「数学を語るのか、数学で語るのか(美杉セミナー '93)」'94年度数学研究会誌38号、三重県高等数学教育研究会(1994)
- [5] 蟹江幸博 「数学的知識の欠如に関する自己認識の調査」三重大学教育学部紀要、第45巻、教育科学(1993),1-13.
- [6] 蟹江幸博、黒木哲徳、中馬悟朗 「数学教育における教師の授業観と意識に関する調査研究」岐阜大学教育学部研究報告(自然科学)、第18-2巻(1993),75-97

- [7] 蟹江幸博「算数綴り方教室の試み」三重大学教育学部紀要、第46巻、教育科学(1994),41-49.
- [8] 蟹江幸博「三角定規の組み合わせ図形の考察」三重大学教育学部紀要、第46巻、教育科学(1994),41-49.
- [9] 蟹江幸博、黒木哲徳、中馬悟朗「小学校教師の数学的常識(仮題)」(未完).
- [10] イアン・スチュアート「スチュアート教授のおもしろ数学入門」(山崎秀記・坂井公・田中裕一訳)日経サイエンス社(1993) Another Fine Math You've Get Me Into ... by Ian Stewart(1992)
- [11] アンドレ・ヴェイユ「アンドレ・ヴェイユ自伝 ある数学者の修業時代」(稲葉延子訳)シュプリンガー・フェアラー東京(1994) Souvenirs d'apprentissage by André Weil(1991)