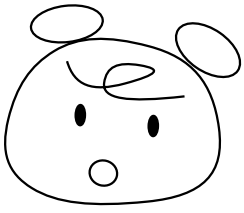
こういうのも数学
（前編）



小澤　嘉康

目 次

1　はじめに

多くの皆様は「数学」という言葉から,「計算」あるいは「日常生活にはあまり関係ない世界」をイメージされるのではないでしょうか？確かに，中学高校で教えられている教科としての数学にはこのような側面があります．しかしながら，あるいは，当然のことですが，本来の数学は中学高校で教えられている数学だけではありません．

今回の「前編」では，数学的な見方をすると多少ものの見え方が変わるような例をいくつか紹介したいと思います．そして，少しでも数学に対するのイメージを変えて頂ければ幸です．数学的な方法には，色々ありますが，今回は「群（ぐん）」（詳しくは後ほど説明します）という考え方を中心に取り上げます．

そして次回の「後編」では，今回準備した「群」の考え方を踏まえて６面パズル（いわゆるルービックキューブ）を数学的に解析する予定です．一見，数学とはあまり関係がないようなおもちゃですが，数学の「群」の構造を上手く入れれば，面白いようにその性質が見えるという点で例としてよく用います．

なお，前編・後編を通して，原則として予備知識を必要といないように心がけました．しかしながら，やはり数学ですから数式や数学用語は出てきます．ですが心配はいりません．一つ一つ順序立てて説明していきますので，慌てずご自分のペースで読んで頂ければ，最後まで読み終えることができます．

各ページの右上にローマ数字のページが付いています．目次と索引をお付けしましたので，よろしければご活用下さい．

2　定義

2.1　集合

数学では，まずはじめに用語の意味を確定します．これを**定義**といいます．日常よく使う用語の場合，人によって既に持っている言葉のイメージがありますので，用語が意味する内容が人それぞれ異なってしまうかもしれません．逆に日常あまり使わない用語の場合，どのような内容なのかよくわかりません．ですので，数学では何よりも先に用語の定義をします．

それでは，まず「集合」と「演算」を定義します．

定義 (集合). これから考えようとする対象を集めたものを**集合**(しゅうごう)といいます．集合は通常アルファベットの大文字を用いて表します．

集合を決めるときの注意点としては，その考える対象に曖昧さがあってはいけません．ある事柄が対象になっているのかどうか人によって判断が異なってしまっては数学になりません．

例えば，物の数を考えようとするときは，数 $0, 1, 2, 3, \cdots$ をはじめに準備しておかなければいけません．これらの数の集合を $\mathbb{N}$（この集合を**自然数の集合**といいます．よく使う集合ですので単に N ではなく $\mathbb{N}$ と強調して書きます.）で表すとすると，

$$\mathbb{N} = \{0, 1, 2, 3, 4, \cdots\}$$

となります．左辺の $\mathbb{N}$ は集合の名前です．右辺では $\{\quad\}$ を書いてその中に具体的にこれから考えようとする対象を書いていきます.（自然数の集合に 0 を入れるか入れないかで好みが分かれますが，0 を入れた方が簡潔になることが多いです.）

考える対象は数だけとは限りません．例えば，ある学校の 4 年 4 組の生徒を考えるとき， 4 年 4 組の生徒全体の集合を P とすれば，

$$P = \{\text{ 青山, 池上, 宇佐見, } \cdots \text{, 若林 }\}$$

となります.

集合をつくる対象の一つ一つ（つまり $\{\quad\}$ の中の一つ一つ）をその集合の**元**(げん)といいます.

ある集合 S において，a が元であるとき，$\boldsymbol{a \in S}$ と書きます．もし b が元でないときは，$\boldsymbol{b \notin S}$ と書きます.

集合 $\mathbb{N}$ では，$0 \in \mathbb{N}$, $3 \in \mathbb{N}$, $32095880 \in \mathbb{N}$ ですが，$-1 \notin \mathbb{N}$, $3.14 \notin \mathbb{N}$ となります.

集合の表し方は，上の例のように $\{\quad\}$ の中に対象を書き上げる方法と，次のように $\{\quad\}$ の中の左に元の型を書き，$\big|$ を引いて，右に元のみたすべき条件を書く方法もあります.

例えば，

$$K = \{s \,\big|\, s \text{ は}\text{K}\text{学校の生徒 }\}$$

とするとき,（もちろん集合 K は K 学校の生徒全体の集合になります）

$$O = \{s \in K \,\big|\, s \text{ は高校 1 年 4 組の生徒 }\}$$

は，〼学校の生徒で高校 1 年 4 組の生徒，つまり，〼高等学校 1 年 4 組の生徒全体の集合になります．

2.2 演算

「集合」が定義できましたので次に「演算」を定義します．

定義 (演算). 集合 G において．集合 G のどの 2 つの元 a と b（つまり $a, b \in G$．a と b は同じでも構いません．）に対しても，唯一(ただひと)つの G の元 c（つまり $c \in G$．c は a や b と同じでも構いません．）が対応するとき，集合 G には**演算(えんざん)が入っている**といいます．この演算を記号 $*$ で表すことにすると，a, b, c の関係は，$\boldsymbol{a * b = c}$ と表すことができます．

例えば，集合 $\mathbb{N}$ には，足し算 $+$ の演算が入っています．どの 2 つの自然数 $a, b \in \mathbb{N}$ に対しても $a+b$ は自然数なので $a+b \in \mathbb{N}$ ですし，その値は唯一つに定まります．しかしながら，集合 $\mathbb{N}$ には，引き算 $-$ の演算は入りません．例えば，自然数 $12, 7 \in \mathbb{N}$ において，$12-7=5$ なので，$12-7 \in \mathbb{N}$ ですが，逆にした $7-12=-5$ は $-5 \notin \mathbb{N}$ ですので「どの 2 つの元に対しても $\mathbb{N}$ の元が対応する」をみたしません．ですので，自然数の集合には引き算は入っていないということになります．

数字以外の元を持つ集合にも演算を入れることができます．例えば，集合 T を

$$T = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$$

とします．このとき，演算 $\boxdot$ を次の表で定義します．

$\boxdot$	$\spadesuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$
$\spadesuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\diamondsuit$
$\heartsuit$	$\diamondsuit$	$\spadesuit$	$\spadesuit$	$\diamondsuit$
$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\clubsuit$	$\heartsuit$
$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$

この表の見方は，例えば，1 行目左から 2 列目は $\spadesuit \boxdot \heartsuit = \heartsuit$，3 行目左から 4 列目は $\clubsuit \boxdot \diamondsuit = \heartsuit$ のようになります．このように集合の 2 つの元に対し 1 つの元を対応させる表を作ることは，その集合に一つの演算を入れることと同じです．

2.3 数の拡張

自然数には引き算は入りませんでした．このまま「引き算はもう考えない」とするか，あるいは制限付きで「大きい数から小さい数の引き算だけ考える」とすることもできます．しかし，どちらにしても計算のルールはあまり簡潔とはいえません．こんなとき数学では「自然数の集合で引き算が入らないなら，引き算が入るように自然数の集合に手を加えればいい」という発想をすることがよくあります．ルールに制限を加えるのではなく，ルールが簡潔になるように考える対象を整え直すのです．多くの場合は，集合の拡張のように広げたり，集合の制限のように狭めたりします．

例えば，自然数の集合を引き算ができるように拡張してみましょう．集合 $\mathbb{Z}$（この集合を**整数の集合**といいます．やはり良く用いるので $\mathbb{Z}$ と強調します．）を，

$$\mathbb{Z} = \{c \,\big|\, c = a - b,\ a \in \mathbb{N},\ b \in \mathbb{N}\}$$

と定義します．説明しますと，$\{\quad\}$ の中の $\big|$ の左側は集合の元の型でした．ここでは c という数が元であることを表しています．この数 c がみたすべき条件を $\big|$ の右側で表しています．ここでは，すべての自然数 a, b に対して $a - b$ を考え，その結果 $a - b$ は自然数でないかもしれませんが，それら全体の集合を $\mathbb{Z}$ としています．0 は自然数ですので特に $b = 0$ とすれば，$\{c \,\big|\, c = a,\ a \in \mathbb{N}\}$ は集合 $\mathbb{N}$ そのものですので，集合 $\mathbb{Z}$ は $\mathbb{N}$ を含んでいます．つまり整数の集合は自然数の集合を引き算ができるように拡張したものになっていることがわかります．

もう少し数の拡張を考えてみましょう．整数の集合には，足し算，引き算の他に掛け算 $\times$ が入っていますね．しかし，割り算 $\div$ は入りません．(念のため集合に演算が入ることの定義を確認して下さい．）ここで，$25 \div 7 = 3 \cdots 4$ のように整数の集合にも割り算があるのではないか？とお思いの方もいらっしゃると思いますが，この式の右辺の $3 \cdots 4$ をよく見て下さい．これは２つの整数でできていますが，整数そのものではないですよね．つまり，$3 \cdots 4 \notin \mathbb{Z}$，つまり整数の集合には割り算は入らないのです．とすると次に考えることは？そう割り算ができる集合を考えるのです．引き算のときに自然数の集合から整数の集合に拡張したときを真似てみましょう．その前に割り算を $\div$ のままでも構わないのですが，例えば，$3 \div 4$ ですと，$c = 0.75$ となりますが，$4 \div 3$ では，$c = 1.3333 \cdots$ となり $\cdots$ のところに曖昧さが残ります．このように割り算の結果を小数で表そうとすると上手くいくときといかないときがあり簡潔では

ないので，$a \div b$ を分数 $\dfrac{a}{b}$ で統一して表すことにします．したがって，

$$\{c \mid c = \frac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z}\}$$

という集合を考えれば良さそうですよね．1 は整数ですので特に $b = 1$ とすれば，$\{c \mid c = a,\ a \in \mathbb{Z}\}$ は集合 $\mathbb{Z}$ そのものですので，この新しい集合は $\mathbb{Z}$ を含んでいます … と，割り算に関しても整数の集合をそのまま拡張できたように思えますが，実はこのままでは大きな問題があります．何でしょうか．細かくいうと 2 箇所ありますが，本質的には 1 つです．それは，割り算のルールで 0 で割ってはいけないということが考慮されていないという点です．つまり，1 つ目は $\{\quad\}$ の中の $c = \dfrac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z}$ では，$b = 0$ を除かなければいけないということ，そして，もう 1 つは，新しく作る集合に 0 を含んではいけないということです．集合に割り算が入っているということはその集合のどの 2 つの数においても割り算ができなければいけないので，集合に 0 を含んではいけないのです．したがって，整数の集合から考えて割り算ができるようにした集合は，

$$\{c \mid c = \frac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z} \text{ ただし } a \neq 0,\ b \neq 0\}$$

となります．この集合は 0 を含んでいないので整数の集合の単純な拡張にはなっていませんが，割り算に関して整数の集合を拡張した集合になっています．ちなみに，この集合に 0 を加えた集合，

$$\mathbb{Q} = \{c \mid c = \frac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z} \text{ ただし } b \neq 0\}$$

を**有理数（ゆうり）の集合**（これも $\mathbb{Q}$ と強調します．）といいます．有理数とは分数そのものです．有理数の集合は整数の集合の拡張になっています．なお，先ほどの，整数の集合から考えて割り算ができるようにした集合は有理数の集合 $\mathbb{Q}$ を割り算ができるように制限した集合と見ることができますので，ここでは，$\mathbb{Q}^\times$ で表すことにします：

$$\mathbb{Q}^\times = \{q \in \mathbb{Q} \mid q \neq 0\} = \{c \mid c = \frac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z} \text{ ただし } a \neq 0,\ b \neq 0\} \quad .$$

3　群

3.1　群の定義

数学での集合とはどのようなものか多少は感じ取って頂けたと思いますのでそろそろ「群」を定義します.

定義 (群). 集合 G において．演算 $*$ が集合 G に入っているとします．このとき，演算 $*$ が次の 3 つの条件

- G のどの 3 つの元 $a, b, c \in G$ においても $\boldsymbol{(a*b)*c=a*(b*c)}$ が成り立つ．(この性質を**結合法則**(けつごうほうそく)といいます．計算は好きなところからして良いという仮定ですので，$(a*b)*c=a*(b*c)=a*b*c$ と書けます.)
- G のすべての元 $a \in G$ に対して $\boldsymbol{a*\varepsilon=\varepsilon*a=a}$ となるような特別な元 $\varepsilon \in G$ が存在する.(この ε を**単位元**(たんいげん)といいます．なお ε はギリシャ文字で e に相等する文字でイプシロンと読みます.)
- G のどの元 $a \in G$ のそれぞれに対し，$\boldsymbol{a*A=A*a=\varepsilon}$ (単位元) となるような元 $A \in G$ が存在する.(この a に対する A を a の**逆元**(ぎゃくげん)といいます.)

をみたすとき，集合 G と演算 $*$ の組 $\boldsymbol{(G, *)}$ あるいは単に $\boldsymbol{G}$ を**群**といいます.

2 つ目条件の $a*\varepsilon=\varepsilon*a$ や，3 つ目の $a*A=A*a$ を見て，当たり前ではないか，と感じた方もいらっしゃるとは思いますが，実はこの性質（**交換法則**(こうかんほうそく)といいます）が成り立たないような例は数多くあります．以下いくつか群の例をあげますので，この点も注目されるとより理解が深まると思います.

3.2　群の例

例 1　整数の集合 $\mathbb{Z}$ で足し算 $+$ を考えると群になります．本当に群であるかどうかは，群の定義をみたすか調べれば良いのです.

まず，前提として $\mathbb{Z}$ に演算 $+$ が入っているのは良いですね．次に結合法則ですが，$a, b, c \in \mathbb{Z}$ とします．$(a+b)+c=a+(b+c)$，これもＯＫです．足し算の単位元

は 0 です．$a+0=0+a=a$ で確かめられます．最後に逆元ですが，a に対しては，$a+(-a)=(-a)+a=0$ ですので $-a$ となります．以上より，$(\mathbb{Z},\ +)$ は群になることが確かめられました．

では，$(\mathbb{Z},\ -)$ はどうでしょうか．演算 $-$ が入っているのは良いですね．そもそも引き算を考えるために自然数の集合から整数の集合を考えたので当たり前です．次に結合法則 $(a-b)-c=a-(b-c)$ が成り立つか確かめてみましょう．これは，例えば $a=3, b=2, c=1$ としてみますと，$(3-2)-1=0$ ですが，$3-(2-1)=2$ ですので，$(3-2)-1\neq 3-(2-1)$ となり，成り立ちません．このように成り立たない例を**反例**(はんれい)といいます．数学では，たとえ $(5-3)-0=5-(3-0)$ のように成り立つ場合があったとしても，反例が一つでもある場合，その性質は成り立たないと考えます．したがって，$(\mathbb{Z},\ -)$ は群にならないことがわかりました．ここで，単位元や逆元は調べないのか？と疑問を持たれた方もいらっしゃると思いますが，そもそも結合法則が成り立たないことがわかったので，後は調べる必要はありません．

せっかく自然数の集合を引き算ができるように拡張して整数の集合を考えたのに，整数の集合は引き算に関して群にならないのでは，群はたいして役に立たないと感じられたかもしれません．ところが，そうではないのです．群を考える一つのメリットは，例えば，整数の集合についていえば，足し算の他に引き算という別の演算を入れようとするのではなく，引き算を足し算と同じだと考えてしまう事なのです．つまり，演算というルールを 2 種類 $(+,\ -)$ 入れるのでなく 1 種類だけで十分だということです．ルールは少ない方が簡潔ですよね．実際どのように考えるのかというと，キーワードは逆元です．例えば，引き算 $7-5$ を足し算 $7+(-5)$ と見るということです．群の定義の逆元の存在とは，結局逆演算を仮定していることと同じ事なのです．

例 2.　有理数の集合に足し算を入れた $(\mathbb{Q},\ +)$ も整数の集合と同様に考えると群になることがわかります．詳しくは練習がてら確認してみてください．

ところが有理数の集合に掛け算を入れた $(\mathbb{Q},\ \times)$ は群になりません．なぜでしょうか．定義を順に確認してみましょう．掛け算が入ることはＯＫです．結合法則も成り立ちます．単位元は 1 で良いですね．逆元は a に対しては $\dfrac{1}{a}$ をとれば，$a\times\dfrac{1}{a}=1$ で良さそうです … と，$(\mathbb{Q},\ \times)$ は群の条件をみたしているように思えます．どこが問題でしょうか？整数の集合から有理数の集合を考えたときのことを思い出してください．そうです，$0\in\mathbb{Q}$ で割ってはいけないのですよね．ということは，逆元の存在が成り立た

ないということです．つまり $0 \in \mathbb{Q}$ に対しては逆元が存在しないので，$(\mathbb{Q}, \times)$ は群にならないという結論になります．

このまま有理数に集合と掛け算において群をもう考えないのはもったいないですね．実は，有理数のうち 0 だけが問題でしたので，先ほど定義した有理数の集合を制限した集合 $\mathbb{Q}^\times$ は群になります．詳しくは確認してみてください．

少し話が脱線しますが，一般にある群において a の逆元を a^{-1} と表すことが良くありますのでそのことについて，ここで軽く触れたいと思います．例えば，$a \times a$ のことを a^2 と書くことはご存じですよね．同様に，$\overbrace{a \times \cdots \times a}^{n\text{個}} = a^n$ と書きます．この記法の性質に，

$$a^m \times a^n = a^{m+n}\,, \qquad (a^m)^n = a^{m \times n}$$

があります．この性質を**指数法則**(しすうほうそく)といいます．m と n は掛け合わせている個数ですので，この指数法則が成り立つことは明らかだと思います．では m や n を整数に拡張したらどうなるでしょうか．つまり a^0 や a^{-1} などをどのように考えたら良いのかということです．よく誤解されますので先に強調しておきますが，はじめから a^0 や a^{-1} の値が決まっているわけではありません．数学では a^0 や a^{-1} の値を**どのように定義しても良い**のです．ただし，その定義の仕方に**合理性**あるいは**整合性**があるということが条件になります．つまり，何かを新しく定義するとき，あるいは，そもそも何を定義するのかは，各自が自由にして良いのですが，今まである事柄に対して，矛盾が生じることだけは絶対に避けなければいけません．数学を勉強していると最初に定義が出てきて，その後定義から色々な性質が導かれていくので，性質より先に定義があるように思われがちですが，実は，数学を研究するときは逆で，先にこんな性質があると良いなと思いながらモゾモゾあれこれやっていくうちに，このように定義すれば良いということに気が付いて，何をどのように定義するかを決めるということが多いです．(でも，モゾモゾしたところを見せるのは格好悪いので定義からはじめる … というわけではありませんよ．)

では実際に個数でない m に対して a^m を定義してみましょう．ここでの合理性とは指数法則が成り立つことです．

まず $m = m + 0$ ですので，指数法則が a^0 でも成り立つようにするとは，

$$a^m = a^{m+0} = a^m \times a^0$$

が成り立つことなので，この両辺を a^m で割ると，

$$1 = a^0$$

となります．ですので，$\boldsymbol{a^0 = 1}$ と定義すると良いことがわかります．ここで，細かいことですが，両辺を a^m で割りましたよね．でも 0 で割ることはできませんので，この定義の仕方では $a \neq 0$ が前提になっています．では $a = 0$ のとき，つまり 0^0 はどうするのか，という疑問が残りますが，実はそう簡単ではないのでここでは省略させて頂きます．

次に m を正の整数とするときの a^{-m} を定義してみましょう．やはり，指数法則が成り立つとすると，$-m = -1 \times m$ ですので，

$$a^{-m} = (a^{-1})^m$$

が成り立つことになります．ですので，a^{-1} を定義すれば良いですね．ここで，

$$0 = 1 - 1$$

ですので，

$$a^0 = a^{1-1} = a^1 \times a^{-1}$$

となりますが，$a^0 = 1,\ a^1 = a$ であることを考慮しますと，

$$1 = a \times a^{-1}$$

となります．両辺に $\dfrac{1}{a}$ を掛けますと，

$$\frac{1}{a} = a^{-1}$$

という関係式が得られました．このことから，

$$\boldsymbol{a^{-1} = \frac{1}{a}}$$

と定義すれば良いことがわかります．ところで，右辺の $\dfrac{1}{a}$ は a の逆元ですよね．ですので，a の逆元を a^{-1} と書くことがあるということです．

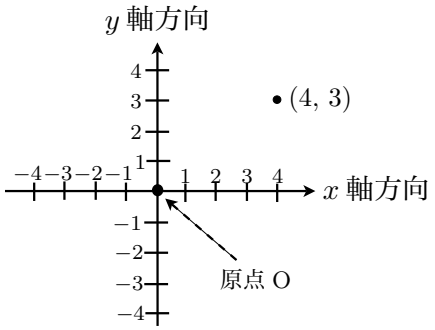
なお，数学はよく自然を記述する言語だといわれますが，それは，数学が持っている合理性あるいは整合性が自然界と非常に相性が良いという意味だと思います．

例 3.　数についての例が続いたので，次は図形を考えてみましょう．中学校で習う図形の合同(ごうどう)も群を用いて表現することができます．

２つの平面図形 **F** と **G** が合同であるとは，一方の図形をその形を変えずに，位置や向きを変えることで，他方の図形にぴったり重ねることができることをいいます．合同の定義ですね．念のため雰囲気では，平面図形ですので，紙でできた２つの図形をつまんで持ち上げるとぴったり重なるときに合同であるということができます．

さて，図形の合同と群とはどのように結びつくのでしょうか？ポイントは，合同の定義で「位置や向きを変える」のところです．図形の「位置や向きを変える」という「操作」（これを**合同変換**といいます）の一つ一つを元に持つ集合を考えると，その集合が群になります．では，詳しく見ていきましょう．

まず，図形の移動を考えますので，それぞれの図形の位置を明確に表さなくてはいけません．そのために**座標**(ざひょう)というものを考えます．これは，平面上を区画整理して住所を与えていくという作業です．どこでも良いのですが基準にする点を決めます．この点を**原点**(げんてん)といい普通 **O** と表します．次に，基準となる原点から基準にする向きを二方向決めます．平面は広がりを持っているので一方向ではうまく区画整理ができません．この基準となる二方向は，どんな向きでも良いのですが，簡潔な方が良いので，互いに 90° になるようにとりましょう．そしてそれぞれ $\boldsymbol{x}$ **軸方向**，$\boldsymbol{y}$ **軸方向**ということにします．最後に，基準になる長さを決めます．本来ならメートルとかインチとか寸など単位が付きますが，それはその時々に必要に応じて付ければ良いので今は単に **1** としましょう．先ほど決めた基準の向き x 軸方向，y 軸方向にそって順に $1, 2, 3, \cdots$ と目盛りをとっていきます．基準の向きと反対の向きに対しては $-1, -2, -3, \cdots$ と負の数で目盛りをとればいいですね．



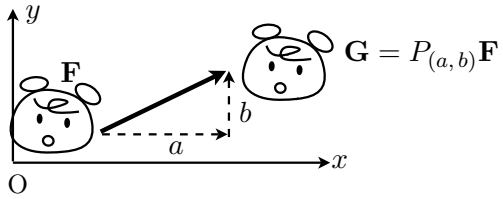
このように座標を入れますと，平面上のすべての場所を数字で表すことができます．例えば図の点ですが，原点から見て x 軸方向に 4，y 軸方向に 3 のところにあるので，この点の場所は２つの数字 4, 3 の組をまとめて (4, 3) で表します．

なお余談ですが，平面上のすべての点はこのように２つの数字の組で表せますので平面の世界は二次元であるといいます．同じように，私たちが暮らしている世界は (縦, 横, 高さ) の３つの数字の組が必要ですので三次元といえます．つまり考えている世界の場所を数字で表すときいくつの数字の組が必要かという数が次元の数になるということです．このように考えれば四次元の世界は決してＳＦだけの話でないことはおわかりですね．ある場所を表すのに４つの数が必要な世界が四次元です．例えば「明日の８時に新大久保」や「１８９１年の麹町」など，つまり時間も付け加えて場所を考えるとそれは四次元になります．

さて，向きや位置を変えること（合同変換のことです）は，次の３つの移動の組合せで表現できます．

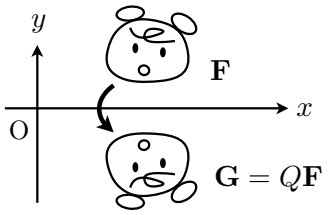
平行移動： 下の図のように図形の向きを変えずに移動します．

x 軸方向に a，y 軸方向に b の平行移動を $\boldsymbol{P_{(a,b)}}$ で表すことにします．



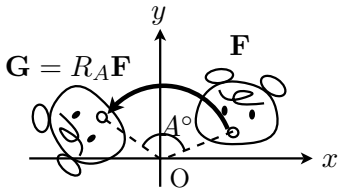
対称移動： あたかも x 軸上にある鏡に映したように移動します．

対称移動を $\boldsymbol{Q}$ で表すことにします．



回転移動： 原点を中心にして左回り（反時計回り）に図形を回します.

角 $A°$ の回転移動を $\boldsymbol{R_A}$ で表すことにします.



ただし，右回りに角 $A°$ は左回りを基準にしますので $-A°$ と考えます．したがって R_{-A} のようになります.

式の書き方ですが，例えば，図形 $\mathbf{F}$ を平行移動 $P_{(a,\,b)}$ で移動した図形を $\mathbf{G}$ とするとき，$\mathbf{G} = P_{(a,\,b)}\mathbf{F}$ のように，元の図形 $\mathbf{F}$ の左側に移動を表す記号 $P_{(a,\,b)}$ を書くことにします．続けていくつもの移動をする合同変換を考えるとき，例えば，平行移動 $P_{(a,\,b)}$ して，回転移動 R_A して，また平行移動 $P_{(c,\,d)}$ して最後に対称移動 Q する，ようなときは，丁寧に書けば，

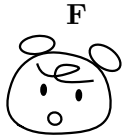
$$\mathbf{G} = Q(P_{(c,\,d)}(R_A(P_{(a,\,b)}\mathbf{F})))$$

のようになりますが，( ) が何重にもなって見づらいので単に，

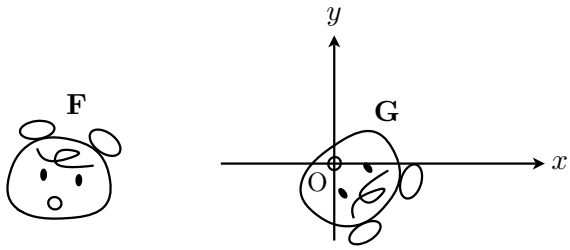
$$\mathbf{G} = QP_{(c,\,d)}R_AP_{(a,\,b)}\mathbf{F}$$

と書きます．このとき，$\mathbf{F}$ から見て左側に順に付け加えるように書いていることに注意して下さい.

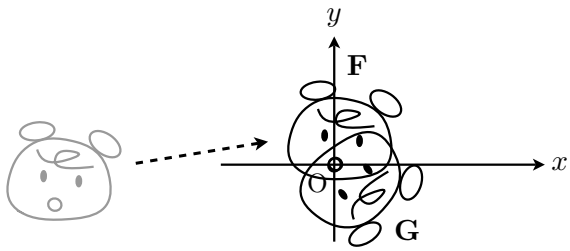
実際に一つやってみましょう.



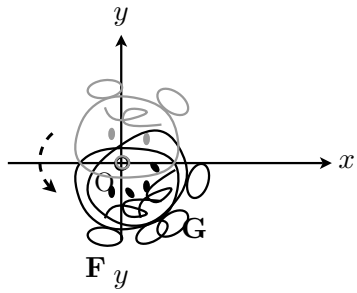
図の２匹のクマ $\mathbf{F}$ と $\mathbf{G}$ は合同ですがどのような合同変換によって移りあうのでしょうか.



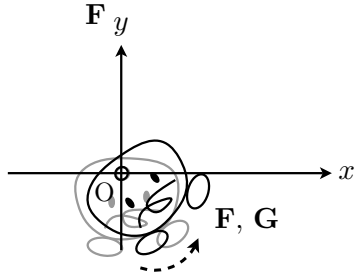
一方のクマ（ここでは **G** の方とします.）のわかりやすいところ（今回は口にします.）を基準にして座標をとります.



まず，他方のクマ（ここでは **F** ですね.）を大雑把に移動します．クマ **F** の口が座標の原点に来るように平行移動 $P_{(a,\,b)}$ をします.



よく見るよ２匹のクマの眉毛の巻き方の向きが逆のようです．そのときは x 軸での対称移動 Q をします.



最後に顔の向きを合わせるために，原点 O を中心とする回転移動 R_A をします.

これより，クマ **F** をクマ **G** に移動するには，

$$G = R_A Q P_{(a,\,b)} F$$

とすれば良いことがわかりました．なお，この移動の仕方は一例です．別の移動の仕方もあるので色々考えてみてください.

さて，いよいよ群になる集合を定義します．合同変換はこれら３種類の移動を組み合わせれば表現できますので，次のような集合

$$\mathcal{C} = \{L \,\big|\, L \text{は}, P_{(a,\,b)},\, Q,\, R_A \text{のいくつかの組合せ}\}$$

を考えます．これより，2つの図形 $\mathbf{F}$ と $\mathbf{G}$ が合同であるとは，$L \in \mathcal{C}$ を用いて $\mathbf{G} = L\mathbf{F}$ を表せることだと定義し直すこともできます．

さて，まず演算ですが，合同変換 $L, M \in \mathcal{C}$ において．図形 $\mathbf{F}$ に対し，$ML\mathbf{F}$ と続けて合同変換を行うと，この図形 $ML\mathbf{F}$ も $\mathbf{F}$ と合同ですので，ML も一つの合同変換を表します．このように「続けて行う」ことを演算と考えます．

次に，結合法則を確かめてみましょう．L, M, $N \in \mathcal{C}$ とします．まず，図形 $\mathbf{F}$ に対し $(ML)\mathbf{F}$ とはどのようなことなのかを確認しておきましょう．確かに $ML \in \mathcal{C}$ なので，別の元 $T \in \mathcal{C}$ を用いて $T = ML$ と表せますので，$(ML)\mathbf{F}$ を図形 $\mathbf{F}$ を一つの合同変換 T で移動した図形 $T\mathbf{F}$ と捉えることができます．しかし一方では，やはり $T = ML$ ですので図形 $\mathbf{F}$ に合同変換 L をして続けて合同変換 M をしたことと同じです．そもそも「続けて行う」ことを演算としていますので当たり前ですね．このことを踏まえますと，

$$N(ML)\mathbf{F} = N((ML)\mathbf{F}) = N(M(L\mathbf{F})) = (NM)(L\mathbf{F}) = (NM)L\mathbf{F}$$

となります．この式変形において図形 $\mathbf{F}$ には特別な条件を付けてはいないのでどんな図形でも成り立ちます．つまり集合 $\mathcal{C}$ の元として，結合法則：

$$N(ML) = (NM)L$$

が成り立つことがわかりました．

単位元は，まったく移動しないという移動です．$P_{(0,\,0)}$ あるいは R_{0° で表現できます．単位元の存在が確かめられましたので，単位元を $\boldsymbol{I}$ で表すことにします．

逆元について．まず個々の移動については，$P_{(a,\,b)}$ の逆元は $P_{(-a,\,-b)}$，Q の逆元は Q そのもの，R_A の逆元は R_{-A} となります．ですので，例えば，合同変換 $L \in \mathcal{C}$ が，

$$L = QP_{(c,\,d)}R_AP_{(a,\,b)}$$

であったとしますと，最後から逆にたどっていけば良いので，L の逆元を M としますと，

$$M = P_{(-a,\,-b)}R_{-A}P_{(-c,\,-d)}Q$$

となります．実際に確かめますと，

$$
\begin{aligned}
ML &= (P_{(-a,\,-b)}R_{-A}P_{(-c,\,-d)}Q)(QP_{(c,\,d)}R_AP_{(a,\,b)}) \\
&= P_{(-a,\,-b)}R_{-A}P_{(-c,\,-d)}(QQ)P_{(c,\,d)}R_AP_{(a,\,b)} \\
&= P_{(-a,\,-b)}R_{-A}P_{(-c,\,-d)}IP_{(c,\,d)}R_AP_{(a,\,b)} \\
&= P_{(-a,\,-b)}R_{-A}(P_{(-c,\,-d)}P_{(c,\,d)})R_AP_{(a,\,b)} \\
&= P_{(-a,\,-b)}R_{-A}IR_AP_{(a,\,b)} \\
&= P_{(-a,\,-b)}(R_{-A}R_A)P_{(a,\,b)} \\
&= P_{(-a,\,-b)}IP_{(a,\,b)} \\
&= P_{(-a,\,-b)}P_{(a,\,b)} \\
&= I
\end{aligned}
$$

となりますので，確かめられました．なお，上の計算で結合法則を用いている事に気が付きましたでしょうか．群の定義に結合法則が必要な理由もおわかり頂けたと思います．

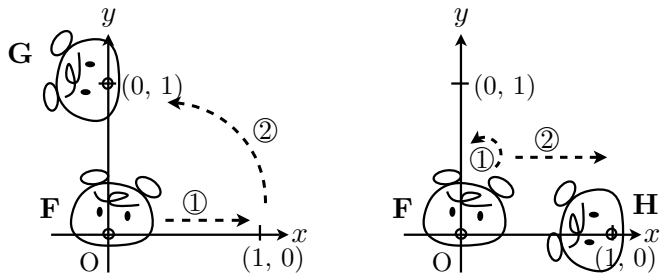
また，この合同変換群には交換法則が成り立ちません．そのことを証明するには，成り立たない例（反例）をあげればいいのですよね．例えば，$R_{90^\circ}P_{(1,\,0)}$ と $P_{(1,\,0)}R_{90^\circ}$ を見てみましょう．下の図でクマ $\mathbf{F}$ の口を基準にしてみます．クマ $\mathbf{G}$ は

$$\mathbf{G} = R_{90^\circ}P_{(1,\,0)}\mathbf{F}\,,$$

つまり① x 軸方向に 1，y 軸方向に 0 の平行移動をして ② 原点を中心に 90° 回転したクマとします．一方，クマ $\mathbf{H}$ は

$$\mathbf{H} = P_{(1,\,0)}R_{90^\circ}\mathbf{F}$$

つまり① 原点を中心に 90° 回転して ② x 軸方向に 1，y 軸方向に 0 の平行移動をしたクマとします．



クマ **G** とクマ **H** は位置が異なりますから $\mathbf{G} \neq \mathbf{H}$ ですね．これより少なくともクマ **F** については，

$$R_{90^\circ} P_{(1,\,0)} \neq P_{(1,\,0)} R_{90^\circ}$$

がいえましたので，一般に交換法則は成り立たないことが証明されました．

例 4.　次は身近な例で席替えを考えてみます．席替えも数学なのか！と驚かれた方もいらっしゃると思いますが，実は数学的に結構重要な内容も含んでいます．是非，一緒にじっくり考えていきましょう．

まず対象とする集合ですが，ここでは，簡単のため担任 Y で生徒数 12 名の学級を考えてみます．

$$\begin{aligned} Y \quad = \quad & \{\, \text{秋葉原, 池袋, 上野, 恵比寿, 大崎, 神田, 五反田,} \\ & \text{新大久保, 高田馬場, 西日暮里, 原宿, 代々木} \,\} \end{aligned}$$

まずこの時点で，今後毎回名前を書くのは面倒なので，例えばイニシャルで，

$$Y = \{a,\, i,\, u,\, e,\, o,\, k,\, g,\, s,\, t,\, n,\, h,\, y\}$$

と書き直すことは良くやることだと思います．これで十分便利なのですが，せっかくですのでもっと考えやすいように，次のように生徒と数字の対応表を作り，

秋葉原	1
池袋	2
上野	3
恵比寿	4
大崎	5
神田	6

五反田	7
新大久保	8
高田馬場	9
西日暮里	10
原宿	11
代々木	12

$$Y = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

とすることができます．ちょうど出席番号を考えていることと同じですね．例えば，新大久保君は 8 番ですし，逆に 10 番といえば西日暮里君であることが明確にわかります．

このように，数学では，考える対象を数字など数学で扱いやすいものに対応させることを頻繁に行います．**一対一対応**とか**同一視**とかいいます．

さて，まず学年始まりは出席番号順に座りますよね．その座席表は次のようだとします．

4	8	12
3	7	11
2	6	10
1	5	9

しばらくたって席替えをしましょう．席順を決める方法はくじでも天の声でも何でも構いませんが,

2	3	8
12	4	5
6	10	1
9	11	7

となったとします．このときの席の移動を分析してみます．まず，各席を区別することからはじめましょう．例えば,「2 列目の前から 3 番目」のように表現することが考えられますが，この場合 2 と 3 の 2 つの数を使うので少し煩わしいですね．(もちろんこのような区別の仕方の方が良いときもたくさんあります.）ですので，ここでは，先ほどの一対一対応の考え方を用いて次のようにしてみます．学年始まりのとき出席番号順に座りました．生徒の数と席の数は同じですので，このとき各生徒が座っていた席を，その生徒の出席番号に対応させます．すると，各席に次のように番号が付きますよね．

4	8	12
3	7	11
2	6	10
1	5	9

これで席の区別を付けることができました．

では，席の移動の分析をしてみましょう．席替えした後の状態を，生徒の出席番号と席の番号を合わせて書いてみますと，

2 (4)	3 (8)	8 (12)
12 (3)	4 (7)	5 (11)
6 (2)	10 (6)	1 (10)
9 (1)	11 (5)	7 (9)

となります．ここで，生徒の番号と席の番号が混ざってはいけませんので，席の番号を ( ) でくくりました．例えば，4 番の生徒は 7 番の席に座っています．席替えによって各生徒がどの席に移ったのか，その対応を生徒の出席番号順に並べてみます．

$$\begin{array}{cccccccccccc} \text{生徒} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \text{席} & 10 & 4 & 8 & 7 & 11 & 2 & 9 & 12 & 1 & 6 & 5 & 2 \end{array}$$

このような対応は頻繁に使いますので ↓ を省略して，

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 4 & 8 & 7 & 11 & 2 & 9 & 12 & 1 & 6 & 5 & 2 \end{pmatrix}$$

のように表すことにします．なお，このような並べ替える対応を**置換**（ちかん）といいます．

しばらくしてから，また席替えをしたとします．今度の席替えの方法は，例えば，

「今 1 番の席に座っている生徒は，今 1 番の生徒が座っている席に移動する」

のようにするとします．これは先の置換 σ において，例えば 7 番の生徒に着目すると，

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & ⑦ & 8 & ⑨ & 10 & 11 & 12 \\ 10 & 4 & 8 & 7 & 11 & 2 & ⑨ & 12 & ① & 6 & 5 & 2 \end{pmatrix}$$

まず $7 \to 9$ なので，9 番の席に移ります．次に 9 番の生徒は $9 \to 1$ で 1 番の席に移っているので，合わせますと，$7 \to 9 \to 1$ と順に移り，結局 1 番の席になることがわかりました．このようにして全員の対応を考えた結果は，

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 7 & 12 & 9 & 5 & 4 & 1 & 2 & 10 & 2 & 11 & 4 \end{pmatrix}$$

となり，新しい席替えに対応する置換 τ が求まりました．なお，この新しい置換 τ は σ を 2 回行ったものですので，

$$\tau = \sigma^2$$

と表すことができます．

ここまでは，席替えに対してそれを表す置換を考えましたが，逆に一つの置換を与えると，それに対応する席替えがあることは明らかですね．例えば置換 ρ を

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 7 & 2 & 10 & 1 & 9 & 4 & 3 & 6 & 11 & 12 & 5 \end{pmatrix}$$

としますと，上の段が生徒の番号で，下の段がその生徒が座る席の番号であることに注意しますと，対応する席替えは，

7	1	11
8	2	10
3	9	4
5	12	6

であることがわかります．(念のため見方を確認しますと，5 番の生徒は 1 番の席に座っています．ここまでいくつかギリシャ文字が出てきたので簡単に．σ は s でシグマ，τ は t でタウ，ρ は r でローです．)

このように，置換と席替えが一対一対応することがわかりました．これは即ち，席替えをすることと置換を考えることとは**数学的に同等**であることを表しています．

なおここまでくればもうおわかりだとは思いますが，席替えをする前の状態，つまり出席番号順に座っている状態（あるいは例えばくじで席替えをしたんだけれども万が一（億が一）の確率で出席番号順になってしまった状態）を表す置換は，

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{pmatrix}$$

ですね．念のため．

さて，いよいよ群の話に入りましょう．もう，お気づきのことでしょうが，これらの置換が群を作ります．まず一番はじめにすることは，考える対象を明確にすることですね．今は 1 から 12 までの 12 個の数字の置換全体を考えますので，これらの集合

を $\boldsymbol{S_{12}}$ で表すことにします．S の右下に小さく 12 と書きましたが，これは 12 個の数字の置換であることを強調したものです．一般に 1 から n までの n 個の数字の置換全体の集合は $\boldsymbol{S_n}$ と表します．

置換 $\alpha \in S_{12}$ とは，1 から 12 までの 12 個の数字すべてを一遍に並べ替えることですが，特に 1 つの数字 p $(1 \leqq p \leqq 12)$ に注目して置換 α によって p が何番目になるのかを表す記号を $\boldsymbol{\alpha(p)}$ とします．すると α は，

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots\cdots & 11 & 12 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) & \cdots\cdots & \alpha(11) & \alpha(12) \end{pmatrix}$$

と表現することもできます．

次に集合 S_{12} に積の演算を定義しましょう．置換は席替えに対応するのですから，2 つの置換 $\alpha, \beta \in S_{12}$ に対して，積 $\beta\alpha$ とは置換 α, β を続けて行うことと定義するのが良いですね．つまり，1 から 12 までのどの数 p に対しても，

$$\beta\alpha(p) = \beta(\alpha(p))$$

であると左辺を右辺で定義します．ここで，α と β の積を合同変換のときと同じように右から左に順に付け加えるように書いていくことにします．この書き方は，実際に上の定義のように数字 p を入れたときに見やすいという利点があります．

例えば，

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 4 & 3 & 6 & 8 & 7 & 9 & 2 & 12 & 11 & 1 & 10 \end{pmatrix}$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 11 & 9 & 3 & 2 & 7 & 1 & 8 & 12 & 5 & 6 & 4 \end{pmatrix}$$

とするとき，積 $\beta\alpha$ は，例えば 1 は

$$1 \xrightarrow{\alpha} 5 \xrightarrow{\beta} 2$$

になります．これを順にすべての数について行うと，(紙面の都合上少し省略しますが)

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & ⑤ & \cdots\cdots & 11 & 12 \\ 10 & 11 & 9 & 3 & ② & \cdots\cdots & 6 & 4 \end{pmatrix} \begin{pmatrix} ① & 2 & 3 & 4 & 5 & \cdots\cdots & 11 & 12 \\ ⑤ & 4 & 3 & 6 & 8 & \cdots\cdots & 1 & 10 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 9 & 7 & 8 & 1 & 12 & 11 & 4 & 6 & 10 & 5 \end{pmatrix}$$

となります.

ちなみに，掛ける順序を交換した $\alpha\beta$ を求めてみますと，

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 1 & 12 & 3 & 4 & 9 & 5 & 2 & 10 & 8 & 7 & 6 \end{pmatrix}$$

となり，

$$\beta\alpha \neq \alpha\beta$$

ですので，交換法則が成り立たないことがわかります.

結合法則はどうでしょうか.「続けて行う」ことを積の定義にしていますが，これは合同変換の積の定義と同じです．ですので，まったく同様にして結合法則が成り立つことを確認することができます．$\alpha, \beta, \gamma \in S_{12}$ と数 $p\,(1 \leqq p \leqq 12)$ において，

$$(\gamma(\beta\alpha))(p) = \gamma((\beta\alpha)(p)) = \gamma(\beta(\alpha(p))) = (\gamma\beta)(\alpha(p)) = ((\gamma\beta)\alpha)(p)$$

となります．数 p には特別な条件を付けていないので，S_{12} の元としての結合法則：

$$\gamma(\beta\alpha) = (\gamma\beta)\alpha$$

が確認できました.

単位元は，まったく変化のない置換ですから，

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{pmatrix}$$

で良いですね.

最後に逆元ですが，置換 $\alpha \in S_{12}$ に注目しますと，数 p は，α によって

$$p \longrightarrow \alpha(p)$$

に移りますが，当然 $\alpha(p)$ は $1 \leqq \alpha(p) \leqq 12$ をみたすわけですから，逆に置換 $\omega \in S_{12}$ として数 $\alpha(p)$ を

$$\alpha(p) \longrightarrow p$$

に移すものを考えれば，ω は α の逆元になります．ここで逆元を表すのに毎回文字を変えるのは煩わしいので，α の逆元を α^{-1} と書くことにします．もう少し具体的に書いてみますと，

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots\cdots & 11 & 12 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) & \cdots\cdots & \alpha(11) & \alpha(12) \end{pmatrix}$$

に対し逆元は，

$$\alpha^{-1} = \begin{pmatrix} \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) & \cdots\cdots & \alpha(11) & \alpha(12) \\ 1 & 2 & 3 & 4 & \cdots\cdots & 11 & 12 \end{pmatrix}$$

ということになります．単に，上の段と下の段を入れ替えれば良いだけですね．ここで，逆元 α^{-1} の上の段が 1 から順に並んでいないが良いのか，と疑問を持たれた方もいらっしゃると思いますが，置換で大事なことは上の段の数字と下の段の数字の対応が明確であることですので，数字の並んでいる順序は本質ではないのです．ただ，実際は数字順に並んでいた方が見やすいので，そのときは必要に応じて並べ替えれば良いでしょう．

以上より，S_{12} は群になることがわかりました．この S_{12} あるいは一般に S_n を**置換群**といいます．

ところで S_{12} の元の数はいくつでしょうか．S_{12} の元の一つ一つが 12 人の席替えに対応しているのですから，元の数は 12 人の並べ方の数と同じです．ですので，12 人の並べ方が何通りなのかを求めれば良いですね．これは中学高校数学では**場合の数**という単元の問題ですので直ぐに求められる方も多いでしょうが少し詳しく見ていきましょう．求め方としましては，1 番の席から順に考えて何人の生徒が座る可能性があるのかを見ていきます．1 番の席には，まだ 12 人全員立っているので 12 通りの可能性が

あります．その 12 人の内 1 人が実際に座ります．次に 2 番の席には，残った 11 人が立っていますので 11 通りの可能性があります．その 11 人の内 1 人が座ります．以下同様にしていきますと，3 番の席は 10 通り，4 番の席は 9 通り，…，11 番の席は 2 通り，そして最後の 12 番目の席は最後まで立っている 1 人が座りますので 1 通りですね．したがいまして，

$$12 \times 11 \times 10 \times \cdots \times 2 \times 1$$

の 479,001,600 通りあることがわかりました．なお，この掛け算 $12 \times \cdots \times 1$ を毎回書くのは面倒なので，この式を **12 !** と書き **12 の階乗**(かいじょう)といいます：

$$12! = 12 \times 11 \times 10 \times \cdots \times 2 \times 1 = 479001600\ .$$

これより，例えばくじなので席替えをしたときに，全員がまったく席が替わらず同じままという確率は，

$$\frac{1}{479001600} \fallingdotseq 0.000000002$$

ですので，まぁほとんど出会えない貴重な出来事だといえるでしょう．

置換群は 6 面パズルの解析に本質的な役割を果たしますので後ほど詳しく取り上げます．

例 5. 最後におまけとして，演算のところで考えたトランプのマークの集合 T は群になっているでしょうか．見てみましょう．

$$T = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$$

⊡	♠	♡	♣	♢
♠	♠	♡	♢	♢
♡	♢	♠	♠	♢
♣	♢	♡	♣	♡
♢	♡	♠	♡	♣

でしたね．演算表がありますので，集合 T に演算 ⊡ が入っていることはＯＫです．では結合法則はどうでしょうか．例えば，♠, ♣, ♡ で見てみましょう．

$$(\spadesuit \boxdot \clubsuit) \boxdot \heartsuit = \diamondsuit \boxdot \heartsuit = \spadesuit$$

ですが,

$$♠ \boxdot (♣ \boxdot ♡) = ♠ \boxdot ♡ = ♡$$

ですので,

$$(♠ \boxdot ♣) \boxdot ♡ \neq ♠ \boxdot (♣ \boxdot ♡)$$

となり，結合法則は成り立ちません．よって，$(T, \boxdot)$ は群にはならないことがわかります.

しかしながら，集合 T に別の演算を入れれば群にすることはできます．例えば,

$$T = \{♠, ♡, ♣, ♢\}$$

⊞	♠	♡	♣	♢
♠	♠	♡	♣	♢
♡	♡	♣	♢	♠
♣	♣	♢	♠	♡
♢	♢	♠	♡	♣

はどうでしょうか．本当に群になっているかを確かめるには，今までのように，結合法則は成り立ってるか？単位元はあるか？どの元にも逆元はあるか？と順に調べていくのも方法の一つですが，ここでは先ほど席替えのところでも用いた「同一視」の考え方を用いた方法を紹介します.

集合 T の 4 つの元を次のように 0, 1, 2, 3 に対応させます.

♠	♡	♣	♢
↕	↕	↕	↕
0	1	2	3

そして，演算 ⊞ に足し算 $+$ を対応させます．ただ新しい集合は $\{0, 1, 2, 3\}$ なので，そのままの足し算では演算になりませんので，２つの元の和が 4 以上になったときは 4 を引くという条件をつけます．例えば，$2+3$ は $2+3=5$ で 4 以上なので $5-4$ より,

$$2 + 3 = 1$$

とします．集合 $\{0, 1, 2, 3\}$ に上の意味での演算 $+$ を入れた演算表を書いてみると,

$\{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

となります．集合 $T = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$ の演算 $\boxplus$ の演算表と比べてどうですか？ちゃんと対応していますよね．なお，この集合 $\{0, 1, 2, 3\}$ は演算 $+$ について群になっていることは，集合の元が数字なので，簡単に確認することができます．マークを数字に置き換えただけなのにこんなに見やすくなるものです．不思議ですね．

ところで，皆様の中には「置き換えると簡単になることはわかるが，では，そもそもどのようにしてこのような対応に気が付いたのか？」という疑問をお持ちの方は少なくないと思います．その答は **$\cdots$ 試行錯誤と感**です！諦めずにできると信じて探求することだ大切です．数学はわかってしまえば簡単なのですが，最初の気が付くところが一番難しいところでもあり一番面白いところでもあります．

なお，この $\{0, 1, 2, 3\}$ にこのような和 $+$ をいれた集合は，整数全体 $\mathbb{Z}$ を 4 で割った余りで分類した集合（この集合のことを**mod（モッド）4の集合**といいます）になっています．ところで，正の整数を 4 で割ったときの余りについては問題ないと思いますが，負の整数を 4 で割ったときの余りとはどのように考えたらいいでしょうか．n を正の整数とするとき，n の中から 4 を取れるだけ取った（q 個取れたとします）後の残りが余り（r とします）ですので，$r = n - 4q$ となります．したがって，

$$n = 4q + r \qquad (\text{もちろん } 0 \leqq r < 3 \text{ ですね})$$

という関係になりますので，正でない整数に対しては，逆にこの関係式をみたす r $(0 \leqq r < 3)$ を余りと定義します．例えば，-7 では，

$$-7 = 4 \times (\mathbf{-2}) + \mathbf{1}$$

ですので，余りは 1 となります．さて，4 で割ったとき余りが 0 つまり割り切れる数（$0, \pm 4, \pm 8, \cdots$ など）を 0 で代表します．同様に 4 で割ったとき余りが 1 になる数（$1, 5, 9, -3, -7, \cdots$ など）を 1 で，余りが 2 になる数（$2, 6, 10, -2, 6, \cdots$ など）を

2 で，余りが 3 になる数（3, 7, 11, −1, 5, ··· など）を 3 で代表します．そうしますと，例えば，2 + 3 は，2 + 3 = 5 ですが，5 は余り 1 ですので，結局 2 + 3 = 1 となります．いくつか例をあげてみますと，

$$1+3(=4)=0, \qquad 3+3(=6)=2, \qquad 1+3+2+2+3(=11)=3$$

などとなります．上の演算表と同じであることは直ぐにわかると思います．数学ではこの mod の集合は何かを分類するときによく用います．

4　置換群

先の群の例で置換群について簡単に触れましたが，置換群は 6 面パズルを数学的に分析するときに中心的な役割を果たしますので，ここでは少しだけ詳しく扱いたいと思います．

先ほどの置換 $\sigma \in S_{12}$ に注目してみましょう．

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 4 & 8 & 7 & 11 & 2 & 9 & 12 & 1 & 6 & 5 & 2 \end{pmatrix}$$

でしたね．まず例えば 1 に注目して順に

$$1 \to 10 \to 6 \to 2 \to 4 \to 7 \to 9 \to 1$$

と追っていきますと，7 回目でもとの 1 が出てきます．これは 1 に置換 σ を 7 回行うと 1 に戻ることを表しています．この流れの途中で出てくる 2, 4, 6, 7, 9, 10 も同じですね．したがいまして，

$$\sigma^7(1)=1, \quad \sigma^7(2)=2, \quad \sigma^7(4)=4, \quad \sigma^7(6)=6$$
$$\sigma^7(7)=7, \quad \sigma^7(9)=9, \quad \sigma^7(10)=10$$

となります．

では次に今出てこなかった数を見てみましょう．3 はどうでしょうか．同様に

$$3 \to 8 \to 12 \to 3$$

となりますので，

$$\sigma^3(3) = 3, \quad \sigma^3(8) = 8, \quad \sigma^3(12) = 12$$

となります．また，

$$5 \to 11 \to 5$$

ですので，

$$\sigma^2(5) = 5, \quad \sigma^2(11) = 11$$

となります．

これですべての数が出揃いました．

このことから何がわかるのかといいますと，例えば 1 は置換 σ を何回行っても 3 にはならないことがわかります．逆も同じで 3 は 1 になりませんね．ということは，この置換 σ において，次の 3 つのグループは

$$1 \to 10 \to 6 \to 2 \to 4 \to 7 \to 9 \to 1$$

$$3 \to 8 \to 12 \to 3$$

$$5 \to 11 \to 5$$

お互いに影響を及ぼさないといえます．ですので，置換 σ をさらに 3 つの置換

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 4 & 6 & 7 & 9 & 10 \\ 10 & 4 & 7 & 2 & 9 & 1 & 6 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 3 & 8 & 12 \\ 8 & 12 & 3 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 5 & 11 \\ 11 & 5 \end{pmatrix}$$

に分解することができます．

ここで各々の置換の見方ですが，例えば σ_1 は数 1, 2, 4, 6, 7, 9, 10 しか出てきませんが，他の数については移動しないと約束します．そうすれば，

$$\sigma_1, \sigma_2, \sigma_3 \in S_{12}$$

であることに矛盾はありません．さらにこの書き方の良いところは，

$$\sigma_1^7 = \sigma_2^3 = \sigma_3^2 = \varepsilon \text{ (単位元)}$$

と表せることです．

このように置換 σ をより性質のわかりやすい $\sigma_1, \sigma_2, \sigma_3$ に分解することで，σ 自体の性質を詳しく見ることができます.

ここで，新しい記号を導入します．置換は，上の段にもとの数，下の段に移る数を書いてその対応関係を表すという書き方ですが，各 $\sigma_1, \sigma_2, \sigma_3$ は順に数が移っていくだけですので,

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 4 & 6 & 7 & 9 & 10 \\ 10 & 4 & 7 & 2 & 9 & 1 & 6 \end{pmatrix} = (1, 10, 6, 2, 4, 7, 9)$$

$$\sigma_2 = \begin{pmatrix} 3 & 8 & 12 \\ 8 & 12 & 3 \end{pmatrix} = (3, 8, 12)$$

$$\sigma_3 = \begin{pmatrix} 5 & 11 \\ 11 & 5 \end{pmatrix} = (5, 11)$$

のように書いても，表していることがわかるので混乱はないですよね.

定義 (互換). 置換のうち，(i, j) のように 2 つの数で構成されている置換を**互換**といいます.

例えば，置換 $\sigma_3 = (5, 11)$ は互換です.

置換群の重要な性質はたくさんありますが，本稿では特に，次回の後編でも用いる次の定理だけ紹介します.

定理. S_n のすべての元は，互換の積で表すことができます.

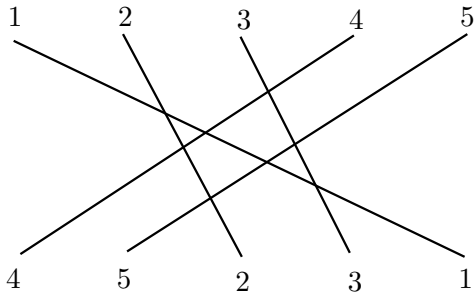
特に，隣り合う 2 つの数の互換 $(i, i+1)$ のみの積で表すことができます.

証明. 本来なら一般の S_n で証明するのですが，煩わしく，わかりにくくなるだけですので，具体的な例で証明をしてみます.

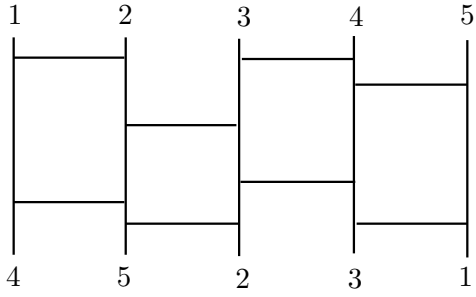
ここでは，置換

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

で見てみましょう．まず，上の段の数と下の段の数で同じものを図のように線で結びます.



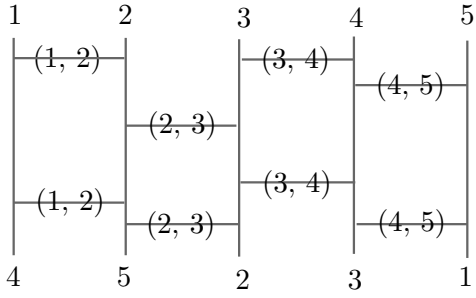
そして，線が交わっているところを丁寧に書き直していくと，次の図のようにできますね.



そうです，**あみだくじ**になります.（つまり，あみだくじも置換の例になっています.）

あみだくじの横線は隣り合う線の交換をするものですので，隣り合う 2 つの数の互換に対応します.

具体的にいいますと，各横線の上に対応する互換を書き込んでみますと，



となります．ここでの注意点としましては，横線に対応する互換には，左から何番目の線を交換しているのかを書いていきます．後は，より下の方から順に書いていきま

すと，

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

となります．これで実際に，置換を互換の積で表すことができました．

一般の置換についても原理は同じですので，同様に表すことができます．

（証明終わり）

5　後編の予告

このあたりで，本稿（前編）は終わりにしたいと思います．次回（後編）ではいよいよ６面パズルの解析を行います．ここでは予告を兼ねてちょっとだけ話の流れを紹介します．

① どのようにしたら６面パズルに数学の群の構造が入るのかを考えます．

② ６面パズルを解くための方法を数学的に考察します．

このとき，はじめから全体を見ると大変なことになるので，大雑把なところから細かいところに視点を移しながら考えます．

③ インチキの見破り方について考えます．

６面パズルの面をグチャグチャにした状態から買ってきたばかりの揃った状態にする方法は①②で得られるのですが，６面パズルを分解して組み立て直したとき，もとの状態に戻せるとは限りません．そのとき戻せないのが，自分の技が未熟だからなのか，それとも，そもそも戻せないのかを見破る方法を考えます．

6　おわりに

普段から数学に深く関わっている方々においても，数学に対するイメージや想いは千差万別ですので，ここに書かれている事柄は私の持っている数学に対する想いでしかないということは強調しておきます．しかしながら，数学の持っている面白味が一人でも多くの方々に伝わりましたなら幸です．

締め切りに追われ，急いで仕上げたところばかりですので，誤字脱字も多く，読みにくいところも多々あり，お恥ずかしい限りですが，最後まで読んで下さいましてありがとうございました．

最後に，原稿の読みにくいところを指摘してくれた，高校 1 年生の数学同好会のメンバーにお礼を申し上げます．

2008.3.11