群論はじめの一歩（1）

1.1　群の定義

G をある集合とし、次の性質を満たす 2 項演算 $\circ$ があるものとする。

（1）演算で閉じている：$x, y \in G$ に対して $x \circ y$ がひとつ決まり $x \circ y \in G$ が成り立つ

（2）結合法則 associativity: $x, y, z \in G$ に対して

$$(x \circ y) \circ z = x \circ (y \circ z)$$ が成り立つ。

（3）単位元 identity の存在: $\exists e \in G$ で、$\forall x \in G$ について $e \circ x = x \circ e = x$ が成り立つ

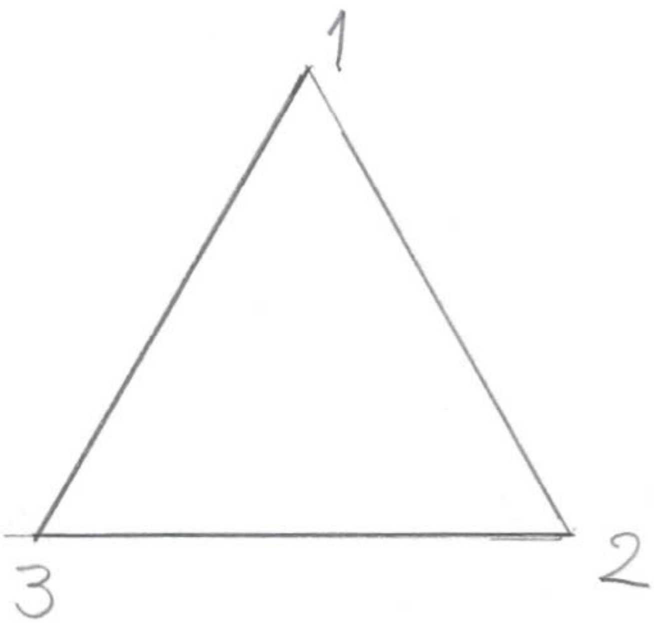
（4）逆元 inverse の存在： $\forall x \in G$ について $\exists y \in G$ で、

$x \circ y = y \circ x = e$ が成り立ち、$y = x^{-1}$ と表す。

この時 $G = (G, \circ)$ を群と呼ぶ。

1.2　群は対称性を測る道具である。3 角形の対称群 S_3

正 3 角形の各頂点に1，2、3という番号がついているとする。



頂点1を固定したまま2と3を入れ替えるには、頂点1から辺23に垂線をおとしその垂線を軸として裏返す（鏡映をとる）ことにより実現できる。これを $(2,3)$ で表す。同じことを他の頂点について行うと $(1,2)$ ，$(1,3)$ が得られる。

これらは鏡映と呼ばれ、鏡映をτ で表すと$\tau\circ\tau=e$ となる。これは$\tau\circ\tau=\tau^2$ とも書かれ、e は何も動かさないことを表す。たとえば、2と3の入れ替えを2回繰り返すことは、結果的にはなにもしないことと同じと考える(恒等変換)。このときτ は位数2を持つという。1,2,3 の入れ替えはほかにはないだろうか？それは$1\to2\to3$ の順に入れ替えるものがある。つまり3角形を時計回りに120° 回転するものである。これを$(1,2,3)$ と表そう。そうすると反時計回りに120° 回転

	説明	逆元	位数
e	単位元	e	1
$(1,2)$	$1\leftrightarrow2$	$(1,2)$	2
$(2,3)$	$2\leftrightarrow3$	$(2,3)$	2
$(1,3)$	$1\leftrightarrow3$	$(1,3)$	2
$(1,2,3)$	時計回り 120° 回転	$(1,3,2)$	3
$(1,3,2)$	反時計回り 120° 回転	$(1,2,3)$	3

するものは$(1,3,2)$と書けるだろう。結局3角形を変えないものは上にあげた

$S_3=\{e,(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}$ という6通りの動かし方がある。

この表において、逆元は、同じ鏡映を2度やると元に戻るので$(1,2)\circ(1,2)=e$ であり、時計回りに120° 回転しそのあと反時計回りに120° 回転すれば、何もしないのと同じであるから$(1,2,3)\circ(1,3,2)=e$が成り立つ。言い換えれば、$(1,2)^{-1}=(1,2)$ 、$(1,2,3)^{-1}=(1,3,2)$などを表している。また元x の位数というのは$x^n=e$ となる最小の自然数n のことである。$(1,2)\circ(1,2)=e$より$(1,2)$ の位数は2であり、120°回転を同じ方向に3回繰り返せば、360° 回転つまり初めの状態に戻るので$(1,2,3)$ の位数は3となる。

1.3 群の例

[例 加法群]

$(\mathbb{Z},+)$ 整数 足し算

$(\mathbb{R},+)$　実数　足し算

$(\mathbb{Q},+)$ 有理数　足し算

これらいずれも　単位元 $e=0$ 、逆元 $x^{-1}=-x$

[例　乗法群]

$(\{\pm1\},\cdot)$　整数で逆数について閉じるもの

$(\mathbb{R}^*,\cdot)$　$\mathbb{R}^*=\mathbb{R}\setminus\{0\}$ 実数からゼロを除いたもの。0での割り算はできないから

$(\mathbb{Q}^*,\cdot)$　$\mathbb{Q}^*=\mathbb{Q}\setminus\{0\}$ 有理数からゼロを除いたもの

これらいずれも単位元 $e=1$、逆元 $x^{-1}=\dfrac{1}{x}$ 文字通り逆数

[例　整数の合同類]

$G=\mathbb{Z}/n=\{0,1,2\cdots,n-1\}$ 整数で n で割ったとき余りが等しい整数を同じと考える。

例) $(\mathbb{Z}/10,+)=\{0,1,2,\cdots,9\}$

$7+5=12=5$ 、$3-9=-6=4$

などとする。

［例　群とならないもの］ $\mathbb{N}$ を自然数とする

$(\mathbb{N},+)$ は 2 の逆元 $-2\notin\mathbb{N}$ がない

$(\mathbb{N},\cdot)$ は 2 の逆元 $\dfrac{1}{2}\notin\mathbb{N}$

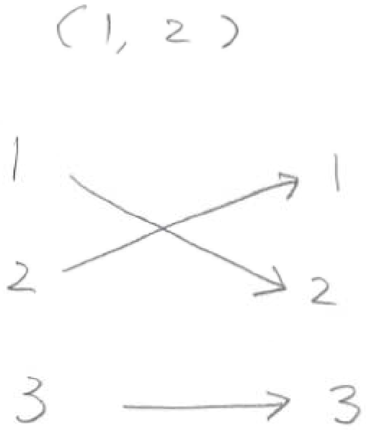
定義　群 $(G,\circ)$ の任意の要素 x,y に対して、$x\circ y=y\circ x$ が成り立つとき G は Abelian

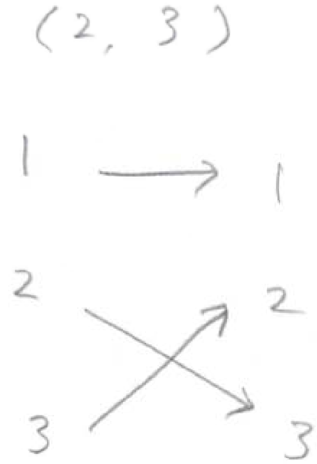
可換群と呼ばれる。

上で上げた S_3 は非可換である。というのは、$(2,3)\circ(1,2)=(132)$

$(1,2)\circ(2,3)=(123)$ となり、演算の順序で結果が異なる。ここで、$(2,3)\circ(1,2)=(132)$

の求め方を示す。





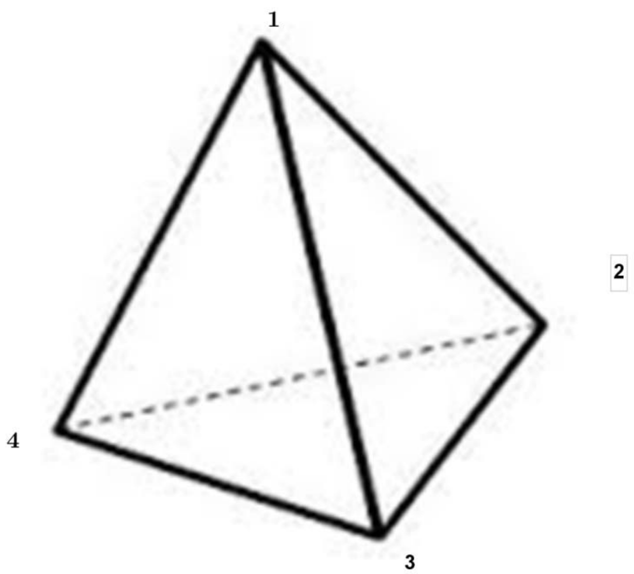
において、$(2,3)\circ(1,2)$ は $(1,2)$ を先に行い、$(2,3)$ を後に行う(順序に注意)

すると、上の図で空白部分をつなげると $1\to2\to3$ 、$2\to1\to3$ 、$3\to3\to2$ を得る。矢印の最初と最後だけ見ると $1\to3$ 、$2\to1$ 、$3\to2$ で、あるいは $1\to3$、$3\to2$、$2\to1$ つまり、$1\to3\to2$ というループが (132) 得られる。

[置換群] 三角形の対称群は頂点の permutation 置換 S_3

$\begin{pmatrix}1 & 2 & 3\\ i_1 & i_2 & i_3\end{pmatrix}$ で、(i_1,i_2,i_3) は $(1,2,3)$ の入れ替えで、$1\to i_1$ 、$2\to i_2$ 、$3\to i_3$ という置換である。上で見たように。異なる置換は6個ある。これは、最初に i_1 を1,2,3から選ぶ(3とおり)次に、残ったものから i_2 を選ぶ(2とおり)、さらに残ったものを考えると i_3 は(1とおりに)決まる。つまり場合の数は $3!=6$ である。一般にの置換 S_n の位数(元の個数)は $n!$ である。

［例　四面体 Tetrahedron］



頂点の置換はS_4　で位数は$|S_4| = 4! = 24$である。

g	$\|g\|$
(1234)	4
(123)	3
(12)	2
$(12)(34)$	2
e	1

(1234)は$1 \to 2 \to 3 \to 4 \to 1$　のようにひとつづつ置き換えていくループで、これは 4 回繰り返すと元に戻る。つまり、$g = (1234)$とおくと、$g^4 = e$　となり、$g^n = e$　となる最小の自然数n　はg　の位数と呼ばれ、それを$|g|$　であらわす。(123)は4　を動かさないで$1 \to 2 \to 3 \to 1$のもの、位数は3、(12)は$3, 4$　は動かさず、$1 \to 2 \to 1$　とするもので位数は2　，

$(12)(34)$は$1 \to 2 \to 1$と$3 \to 4 \to 3$　となる 2 つのループで位数は2である。

$|g|$　の値は群の位数$|S_4| = 4! = 24$の約数になっていることを注意しておこう。

また、S_4 は非可換群である。なぜならS_4 のうち4を 動かさないものについて考えると $(2,3)\circ(1,2)$と$(1,2)\circ(2,3)$があるが$(2,3)\circ(1,2)\neq(1,2)\circ(2,3)$は$S_3$ においてすでに示したものである。同様に考えると、S_n，$n\geq 3$ はすべて非可換群である。

1.4 単位元、逆元の一意性

消去法則 $x\circ y=x\circ z$ が成り立てば、$y=z$ $y\circ x=z\circ x$ が成り立てば、$y=z$

$x\circ y=x\circ z$において、左からx^{-1} をかけると$x^{-1}\circ(x\circ y)=x^{-1}\circ(x\circ z)$

結合法則より、$(x^{-1}\circ x)\circ y=(x^{-1}\circ x)\circ z$となるが$(\ \ )$ のなかは、単位元であるから、

$y=z$がわかる。■

単位元の一意性：

単位元が２つe_1,e_2 があるとする。$x\circ e_1=x$ 、$x\circ e_2=x$ が成立するが、右辺が等しいので、$x\circ e_1=x\circ e_2$ が成り立つ。したがって、消去法則から$e_1=e_2$ がわかる。■

逆元の一意性：

x^{-1} としてa,b 2つあったとする。$a\circ x=e$ 、$b\circ x=e$ であるが右辺が等しいことから、
$a\circ x=b\circ x$ が成り立つ。したがって、消去法則より$a=b$ がわかる。■