群論入門　1

―群の用語と基礎概念―

（p436-p443）

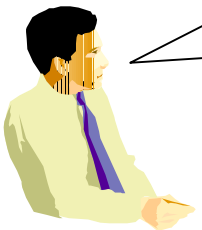
群論とは何か？

群論とは1829年、当時まだ高卒だった
フランスのエヴァリスト･ガロアが創始した数学の一分野です。

ガロアは天才すぎて2度も大学入試に失敗、
その後革命家として2回、逮捕され、21歳で決闘で死亡。

論文を2回も無視され、3回目はポアソンの 理解できない」
という返事に失望したのね。

ガロアは決闘前夜、友達に手紙を書き、群論の考えを伝えた。
僕にはもう時間がない」が何度も繰り返され、読む人の心を打つ。



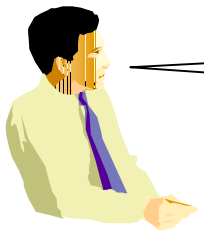
ところで、群論とは何か？

おっと、ガロアの生涯があまりにドラマチックなので…。
すまんすまん。
群論とは **群**（Group）」の性質を研究する学問です。

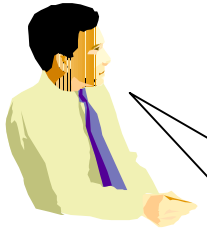
群」とはある4条件を満たすもののことです。

その4条件とは
演算が閉じていること」
結合法則」
単位元の存在」
逆元の存在」
です。

ところで、**血液型占い**に興味はありますか？

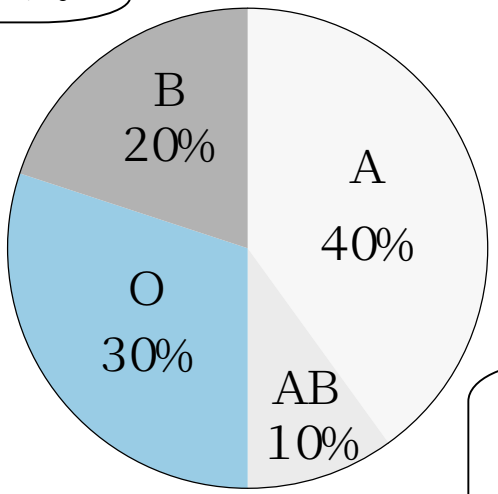


日本人の血液型分布と血液型占い



B型は**逆**を行きたがります。
よく仲間外れになります。

B型



規則を守って
はみ出さない
それがA型

A型

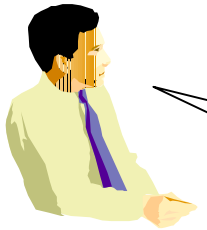
O型って、
いつもみんなの
中心にいるの

O型

AB型のヒトは
人と人との
関係を取り持つ
のが上手いの

AB型

次の4条件を満たせば「群」です



B型

元 a の逆元は a^{-1} と書く。
$a \star a^{-1} = e$（右逆元）
$a^{-1} \star a = e$（左逆元）
となるような a^{-1} が逆元。

たとえば整数の足し算なら
$a + (-a) = 0$（単位元）
つまり $-a$ が**逆元**だね。

A型

整数と整数は
「足し算」でやはり整数になる。

つまり「**閉じている**」し、
結果は1通りに定まるね。

A　閉じた演算が定義されており、結果が一意に定まること
AB　結合法則が満たされること
O　単位元があること
B　逆元があること

O型

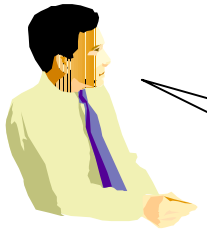
単位元って、どんな元 a に対しても
$a \star e = a$（右単位元）
$e \star a = a$（左単位元）
となる元 e のことよ。たとえば整数の足し算なら
$a + 0 = a$
$0 + a = a$
だから0が**単位元**になるの。

AB型

$(A \star B) \star C = A \star (B \star C)$
ってことね。たとえば
$(a + b) + c = a + (b + c)$

これを「**結合的**」っていうの。

4条件のうちいくつか欠けると「半群」・「モノイド」



B型

{1, 2, 3, 4}から2つ選び、
大きな方を残すことを演算としよう。
この場合、1が単位元。
でも、たとえば2には逆元がない。
これを**モノイド**っていうんだ。

いくつかの演算が定義された集合を
代数系っていう。

半群もモノイドも群も代数系だ。

A型

モノイド { **A 閉じた演算**
AB 結合法則
O 単位元
B 逆元 } 半群

O型

たとえば正の偶数
{2, 4, 6…}と足し算は「半群」。

単位元（0）がないでしょ？
逆元（負の数）もないし。

代数系を表記するときは
集合と演算をカッコ内に並べるの。

たとえば
（整数, ＋） とか
（{1, 2, 3, 4}, Max） とかね。

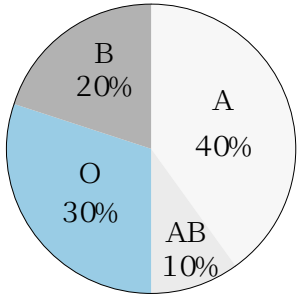
AB型

半群・モノイドの覚え方

モノイド

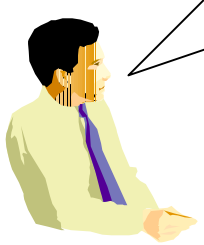
A　閉じた演算
AB　結合法則
O　単位元
B　逆元

半群



群の条件　　血液型

B型って、はみ出しやすいだろ？
B型の法則がない、つまり
群の4条件のうち
「逆元がない」ものがモノイドなんだ。



AとAB型で日本人の50%。
だから **半**　群。

あっ、怒らないで…。

「元」「位数」「有限群」「無限群」

群に慣れるために、いろんな具体例を見ていこう。

その前に**用語の説明**。

群Gのメンバーのことを **元**」(element)。
メンバー数を **位数** (order)」っていう。
位数は **＃G** とか **｜G｜** と書く。

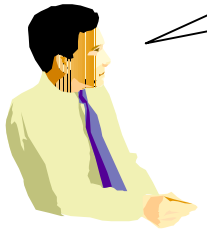
位数が有限なら **有限群**」(finite group)
位数が無限なら **無限群**」(infinite group)。
無限群の位数を＃G=∞ って書いていいの。

ちなみに
単位元は **unit element** もしくは **identity element**。
逆元は **inverse element**。
群論は **Theory of Groups** よ。

ー群の具体例をいくつかー

たとえば整数の集合は足し算で群をなす。
単位元は0で、nの逆元は－n。

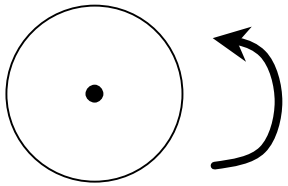
整数はかけ算において群をなさない。
たとえば **3の逆元は1／3で、整数として閉じてない**だろ？



正の実数はかけ算で群よ。
単位元は1、aの逆元は1／a。

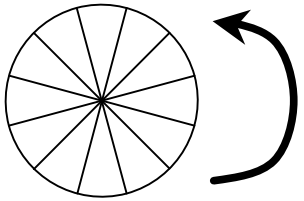
群の演算のことをしばしば **積**」っていうの。
足し算でも **積**」。ガマンして。
英語は product。

－群の用語－　円の群・法nの群



円のn度の回転も群だ。これを**回転群** (rotation group) という。
単位元は「静止」。a度の回転の逆元は－a。これは無限群だね。

回転の角度を(360／n)度に
制限すれば、位数nの回転群になる。
群マシンで、n=12の場合を確かめよう。



n=12の例

群マシンで確かめてほしいけど、
a回転＋b回転＝b回転＋a回転
でしょ？
一般に **a★b=b★aが成り立つ群**を
可換群 (commutative group)とか
アーベル群 (abelian group)
っていうの。

アーベルはノルウェーの、ガロアと同じくらい悲劇的な天才数学者よ。
ノルウェーでは英雄で、500クローネ札（ 3万円）になってんだって！

(360/n)度の回転群は、
(a+b)をnで割った演算そのもの。
だから元が1～(n－1)で、
nを法とする (modulo n)
整数の集合も群なの。

modulo って、small measure って意味よ。
大きな数 たとえば187)を
小さなものさし たとえば12)で測るのね。

クラインの 4元群　その 3

2項演算 (binary operation)の結果を
表にしたものを
乗積表（じょうせきひょう）」っていうの。
英語は multiplication table。

群なら **群表**」(group table)
って言ってもいいわ。

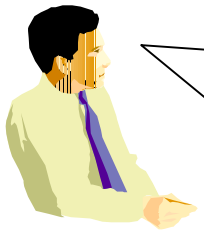
群表が対角線に対称なら、
それは**アーベル群**なの。

群表からわかるとおり、
4を法とする群は**アーベル群**だ

群表

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

対称！



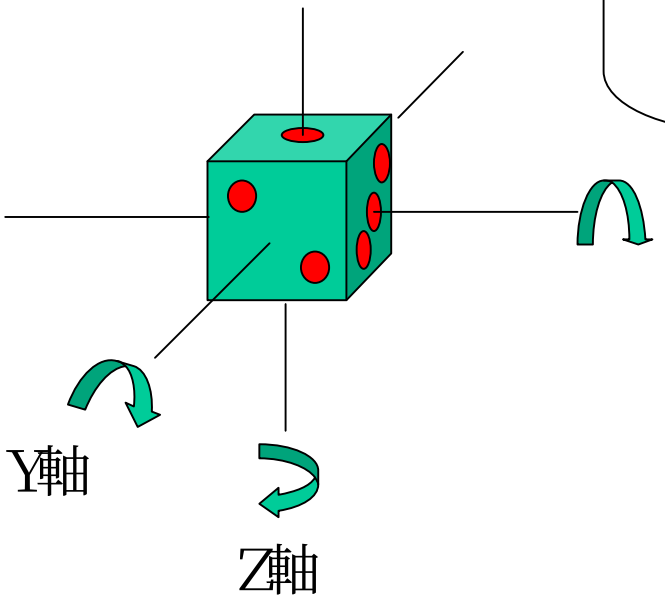
群マシンは、
有限のアーベル群なら
取り扱えるんだよ！

ちょっと誇大広告だけど…
今は見逃してあげるわ。

クラインの 4元群　その 1

サイコロを **180度** 回転させる方法は、
x軸、y軸、z軸の 3通りあるね。
それと0度の回転（静止）も立派な回転だ。

この 4つの元を**クラインの 4元群**
(Klein's Four Group) という

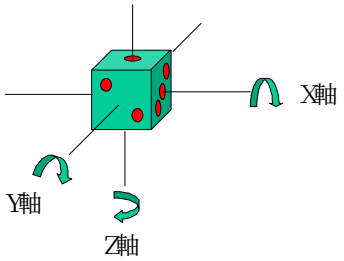


それぞれの回転を
x, y, z, e（静止）
と書きます。

クライン(Felix Klein 1989－1925・ドイツ)って、
幾何学を群論で再構成したことで有名な数学者よ。
ほかの業績は楕円モジュラー関数論…なんだって。

クラインの 4元群　その 2

クラインの 4元群の**群表**よ。



2手目（2項演算の右）

1手目（2項演算の左）

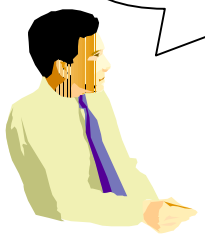
	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

X軸回転＋Y軸回
は、なんと
Z軸回転
に等しい！

試してみよう！

くどいけど、あくまで
180度回転の話だよ。

同じ180度回転を
2回続けると
静止と等しい。



乗積表から、群かどうかをチェックする

B　逆元があること

単位元の行・列が
ちゃんと
埋まっていること。

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

A　閉じた演算で、結果が一意

どの文字も**いちばん上の行**のどこかにあって、
同じ文字は同じ行・列に再び現れないこと。
（さもないと逆演算が一意でなくなる）

	e	x	y	z
e	e	x	y	z
x	[redacted]			
y	y	z	e	x
z	z	y	x	e

O　単位元があること

	e	x	y	z
e	[redacted]			
x	[redacted]			
y	x	e	z	y
z	y	z	e	x
	z	y	x	e

いちばん上と
同じ行がただ1つ、あるはずなのね。
その行が単位元よ。

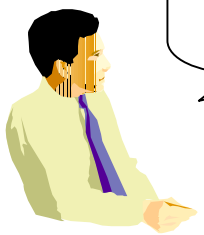
AB　結合法則が満たされること

うまい方法がないの。
1つずつ確認してね。

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

結合法則のチェックは難しい

○ **B　逆元があること**



単位元 ⑴の行・列が
埋まっている。
いいね、いいね。

○ **A　閉じた演算で、結果が一意**

乘積表

	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	1	5	2	4
4	4	5	1	3	2
5	5	4	2	1	3

同じ文字は
同じ行・列に
再び現れない。
良さそうだね。

いちばん上と同じ行…
あった！　「1」の行ね。
これが単位元。OKよ！

(2③)2 = 42 = 5
2 (32) = 21 = 2

結合法則でアウト!
ね、難しいでしょ？

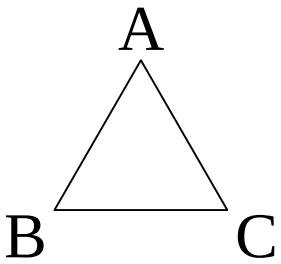
○ **O　単位元があること**

× **AB　結合法則が満たされること**

群」に慣れよう　(正三角形の群)

別の群を見てみよう。**正三角形の回転群**と言われるものだ。

この正三角形の形を変えない操作は、全部で6つよ。

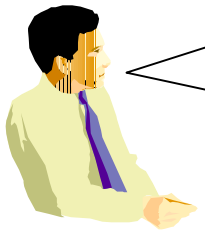


静止をe、
時計と反対周りの60度回転をp、
A軸での折り返しをqとすると、

e
p
p^2
q
pq
p^2q

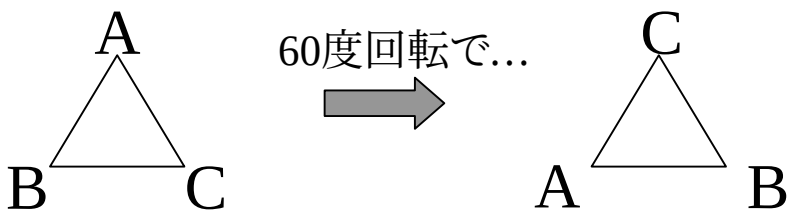
と書ける。

静止、
60度回転、
120度回転、
軸Aでの折り返し、
軸Bでの折り返し、
軸Cでの折り返し。
…この6つね。



(注)一般に、正n角形の群の位数は2n。(回転がn個と、折り返してからの回転がn個)

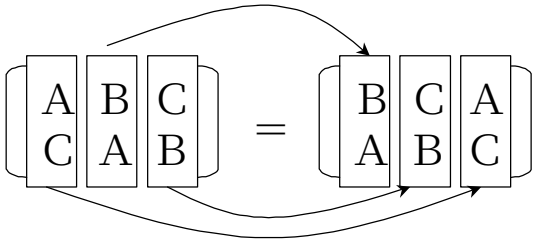
置換 (permutation)の 2行表記



A B C	演算の**前**
C A B	演算の**後**

60度回転 pによって、
Aは C、Bは A、Cは Bとなる。
このとき回転 pは左のように書く。

『どこが」『どこに」移ったかさえ
合っていればいいの。
だから
列ごとに入れ替えても
イコールで結んでOK！



退屈な方に…ひまつぶしコーナー！
出典は主にヴィルチェンコ編 数学名言集」大竹出版。

数学は潜在的に自然より豊かだ。
可能性が現実より豊かであるように。
ーピスメンー

2行表記の積、単位元、逆元

p（60度回転） q（A軸での折り返し）

$$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \times \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$\| $$

$$\begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} & \boldsymbol{C} \\ C & A & B \end{pmatrix} \times \begin{pmatrix} C & A & B \\ \boldsymbol{B} & \boldsymbol{A} & \boldsymbol{C} \end{pmatrix}$$

$$\| $$

$$\begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} & \boldsymbol{C} \\ \boldsymbol{B} & \boldsymbol{A} & \boldsymbol{C} \end{pmatrix}$$

2つの置換の積、
たとえばpqの計算は、
左のように行う。

第1元の下の行と、
第2元の上の行を
合わせるのがポイント。

$$p = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \quad \rightarrow \quad p^{-1} = \begin{pmatrix} C & A & B \\ A & B & C \end{pmatrix}$$

$$e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

逆元は、1行と2行をひっくりかえすの。
単位元は上下同じよ。

「大学進学」は
数式だと、こうかな？

$$\begin{pmatrix} \text{数} & \text{物} & \text{国} \\ \text{物} & \text{化} & \text{数} \end{pmatrix}$$

君らが高校で習った数学は、実は物理だったのだ。
君らが高校で習った物理は、実は化学だったのだ。
では数学はどこで習ったか？　実は国語だったんだねぇ！
－東工大の数学科に代々伝わる言葉－

1行表記

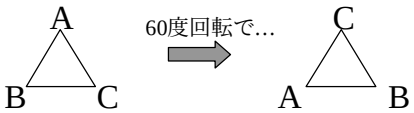
アルファベットの sと tを入れ替える置換は、
2行表記だと

$$\begin{pmatrix} abcdefghijklmnopqrstuvwxyz \\ abcdefghijklmnopqrtsuvwxyz \end{pmatrix}$$

長いし読みづらい！

だから1行表記が普通よ。たとえばこの場合、(st) って書くの。
正三角形の60度回転 pなら (ACB)。 Aは C、Cは B、そして Bは Aってこと。

(ACB) = (CBA) = (BAC) だけど、(ACB) ≠ (ABC)。わかる？
…あ、**単位元 eは (1)** って書くのね。



p (90度回転)

$$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

数学が難しいのは、複雑だからではなく、
概念の極端な単純化についていけないせいなのだ。
だから普通の人は、数学の単純な概念を、
より複雑な具体例にすると理解できる。
―どこかの本（忘れた）―

n次の対称群

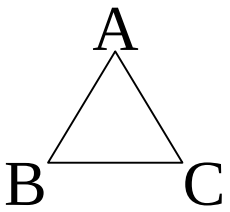
1～nを入れ替える置換を**すべて**集めたものを、
n次の対称群 (**S**ymmetric group)っていって、 S_n って書くの。

位数は　n! 個　よ。なぜって？　2行表記で考えて。
下の行に、1～nを好きに並べていいから。

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$$

$n!$

実は**正三角形の群は、3次の対称群 S_3 と等しい**。
どちらも3文字で、位数6だろ？



$= \quad S_3$

2つしか入れ替えないものを**互換** (transposition) といいます。
たとえば (13) は**互換です**し、
(123) は互換**ではありません。**

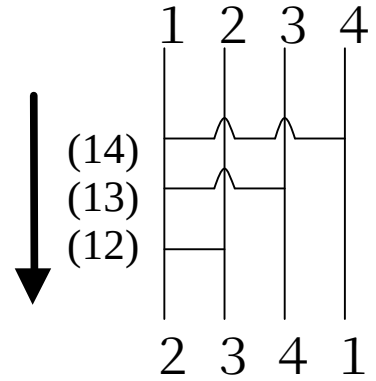
数学、それはなるべく計算を避けるための技術だと言える。

―マクラミン―

互換 ・偶置換 ・奇置換

どんな**n次の置換も**
互換の積であらわせます。
たとえば（1234）＝（12）（13）（14）。

順序に注意！



アミダクジの場合、1本の横線が 1つの互換になる。
どんな置換もアミダクジで表現できることになる。

置換が偶数個の互換の積になれば**偶置換、**(even permutation)
奇数なら**奇置換**(odd permutation)です。
たとえば（13）は奇置換、（123）＝（13）（12）なので偶置換。

僕「二乗するとマイナスになる数もあるんだよ」
斉藤「オレは目に見えないものは信じない」
僕「そりゃムチャクチャだ。たとえば素粒子は…」
斉藤「じゃあオレが女だって言ったら信じるか？」
僕「いや」
斉藤「どうすれば信じる？」
僕「やっぱ…見せてもらわないと」
斉藤「そうだろう?」

―元落語研究会部長、斉藤俊崇くんと僕の会話から―

交代群を群カードからつくる

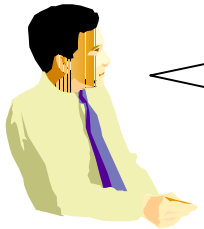
ワンポイント英単語（笑）

alter＝＝「他」(ラテン語)。
この言葉関連は・・・

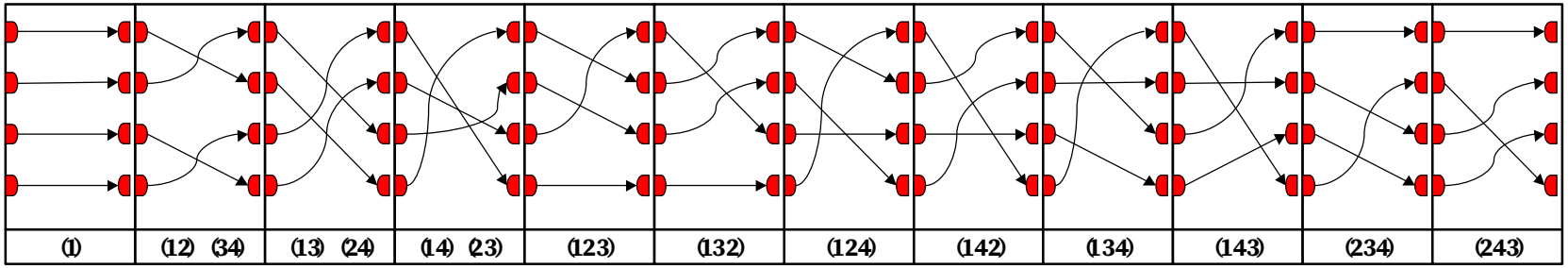
altruists（利他主義者）
altruism（利他主義）
alternate（1つおき＝1つ飛ばして他のもの）
alternate（代理人）
alternative（代替案）
alteration（変化＝なにかを別のものに変える）
alter（変更する）
altercation（口論＝別の意見を持つから）
alter ego（次の親友＝もう1人のあなた）

n次の対称群のうち **偶置換だけ** 集めたものを
交代群 (alternating group) といい、A_n と書きます。

4次の対称群、つまりS_4で考えよう。
群カード、持っているかな？
24枚（× 2組）あるよね。
どのカードがA_4の元だろう?
いいかえれば、**偶置換はどれ？**



正解は↓の12枚。（1）も立派な偶置換さ。
偶置換は交点がみんな偶数個だよ！
逆も成り立つ。奇置換は交点が奇数なんだ。



単位元

対称群、交代群の覚え方　その１

なぜ**対称群**とか**交代群**って呼ぶの？　覚えにくいわ…。

ab+**b**c+c**a**　は　置換　(ab)　を行っても

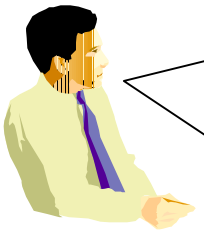
ba+**a**c+c**b**　となって、値は変わらない。
こういうのを **対称式** (symmetric expression) という。

対称式の値を変えない置換の集合が　**対称群」だ。**

(**a**-***b***)(**a**-c)(***b***-c)は 置換 (ab) で

(**b**-***a***)(**b**-c)(***a***-c)となり **符号が交代してしまう。**
これを**交代式** (alternating expression) という。

交代式の値も変えない置換の集合が　交代群」だ。



たとえば偶置換の 1つ　(abc)　では、
(**a**-***b***)(**a**-c) (***b***-c)は

(**b**-***c***) (**b**-a) (***c***-a)。値は変わってないよ。

対称群、交代群の覚え方　その２

なぜ**偶置換**は**交代式の値を変えない**の？

1回の**互換**で符号が切り替わるから、
偶数回の**互換**をする偶置換は、
交代式の値を変えないのよ。

一般に、対称式を変えないのは易しいが、
交代式を変えないのは難しい。
だから交代群は、いわばエリート揃い。
エリートだからメンバー数、つまり位数も少ない。

群だって少しでも高度な機能を宣伝したい。
「オレは交代式でさえ値を変えないゼ」って
威張っているエリートが　**「交代群」**、
私は対称式なら大丈夫ですが…」っていう庶民が　**「対称群」**。

まあ、こう覚えれば忘れないよ。

1章の終わり

群の元は、数である必要はない！
たとえば回転という**運動**でもいいし、
置換という**行為**でもいいんだ。

演算は、足し算やかけ算、いえ、
普通の算術の「演算」である必要すらないわ。
1つの行為が他の行為に**引き続く**
といった種類の「演算」であればいいの。

もはや数学は数だけに仕えない！
この洞察こそガロアの天才であり、
そして悲劇の原因だった。

それではひとまずお別れしましょう。
また会えるかしら？

伊藤智義 作／森田信吾 絵 **栄光なき天才たち1**』集英社、1987