東海女子大学紀要，12，1992

置換群の電算機計算
——置換群の電算機計算とその応用——

谷村　義勝

§1　はじめに

電算機（computer）は、電卓（caluculater）とは異なり、計算手順をプログラムとして与えると、高速に複雑な計算を、自動的に処理することができる。私は過去の拙稿で、電算機のもつこの機能を活用し、数論における未解決問題、２次体問題等の解明を試みた。しかし、他の面で電算機は、多くのシステムの膨大なデータを記憶すると共に、それらを即座に分析比較する機能をも有している。これが、「情報化社会」の立役者と言われる理由もここにある。さて、現在の数学の分野は多様化し、計算結果の求答のみで解決が不可能なものが多くなった。例えば論理数学、代数系論（集合論、群論、イデアル論等）がそれである。しかし、「はじめに群ありき」と言われるように、群の概念がそれ等の中核である。一般代数系の電算機的な研究は、近頃内外の研究機関で実施されるようになったが、それらではある程度の数学論理記号、言語を理解する高性能の機器を利用する所が多い。また業績発表もなされているが、内容は特殊で専門的な分野である。

そこで私はPersonal computerの限定使用によって、一般群の基礎となる置換群の解析を試みたい。また本稿ではとくに、ガロア群とアーベル群がどのように置換群と関連するかを明らかにするとともに、それと代数方程式の解法との関連を考えることにする。

§2　置換群

2．1　群について

集合Gをある元素の集合とし、Gが次の４つの公理をみたすとき、これを群という。（元素を以下「元」と略称する。）

(I)　Gの任意の元a、bに対して、ある結合○が定義されて、$a\circ b$がただ１通りにGの元として定まる。

(II)　Gの任意の元a、b、cに対して
$(a\circ b)\ \circ c=a\circ\ (b\circ c)$
が成立する。（結合法則）

(III)　Gに適当な元eがあり、Gのどの元aに対しても　$e\circ a=a$　が成り立つ。
（eをaの単位元という。）

(IV)　Gの任意の元aに対して、$x\circ a=e$となるようなxがGに存在する。
（このxを aの逆元とよびa^{-1}とかく。）

（註）

(1)　とくにGの任意の元a、bに対して
$a\circ b=b\circ a$　が成り立つとき、Gを可換群またはアーベル群とよぶ。

(2)　群の元の個数をその群の位数とよぶ。

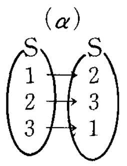
(3)　群論における結合○は、通常は乗法とみなされるが、加法とみてもよい。また特別に定義されることもある。

2．2　置換群

群の歴史は、置換群の歴史に源を発してい

る。群の概念を捨象した「おきかえ」、「並べかえ」の日常算術（順列）も重要で、興味ある要素を多く持っている。ゲームの本質も、これらと確率の交錯であろう。

いま、（1，2，3）の３数字をおきかえると、１２３、１３２、２１３、２３１、３１２、３２１、の６数字が得られる。つまり$3!=6$が３個の相異なる数字の総順列である。４個、５個の相異なる数字に対しては、総順列はそれぞれ、$4!=24$、$5!=120$　となる。一般に n個に対しては$n!$個の総順列が得られる。



いま思考を抽象化しＳを、元が１，２，３であるような集合とし、Ｓ＝{１，２，３}とかき、ＳからＳへの全単射（ＳからＳの上への１対１の対応）を考える。例えば左図の全単射をαとすれば、αによって、１→２、２→３、３→１が対応するから$\alpha(1)=2$、$\alpha(2)=3$、$\alpha(3)=1$、とかくことができる。ついでβ、γ、……と他の対応を指定すれば、Ｓの元はそのままであるような同型対応（同型射像）が６通りあることがわかる。これらの対応を

$$\alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}、\quad \beta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}、\quad \cdots\cdots$$

などと書くことにする。

なお、この対応の積であるが、α、βを用いると、$\alpha(1)=2$、$\beta(2)=1$、$\alpha(2)=3$、$\beta(3)=3$、$\alpha(3)=1$、$\beta(1)=2$　となるから、１→１、２→３、３→２、の対応が得られる。これを行列表現すると、

$$\alpha\beta=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

となり、結果もひとつの対応である。また、1、2、3をそれ自身に対応させる対応とともに、任意の対応について（例えばαに対して）

$$\alpha\alpha^{-1}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

のような「逆対応」α^{-1}が存在する。そのほか、この場合の６つの対応の集合においては、群の４つの公理がみたされる。この群を３次の対称群（または置換群）とよび、Ｓ(３)で表すことにする。一般にn次対称群をＳ(n)とかく。

２．３　偶順列と奇順列

１、２、３　の３数の順列は、１２３、１３２、２１３、２３１、３１２、３２１の６通りである。いまこの中での順列abcで$a<b<c$のとき、abcの「転倒」は０という。１３２は３↔２で転倒があるから転倒１である。また２３１は、２↔１、３↔１の逆順より、転倒２となる。３２１は、３↔２、３↔１、２↔１で３個の転倒数（最多）を有している。以上は３個の数であったが、数字が多くなると転倒数の計算が面倒である。一般にn個の連続する数字〔１２３……n〕を、他のn個の連続する数字の順列〔$a_1a_2a_3\cdots\cdots a_n$〕に変換する置換を、

$$\alpha=\begin{pmatrix}1\ 2\ 3\cdots\cdots n\\a_1\ a_2\ a_3\cdots\cdots a_n\end{pmatrix}$$

とかき、〔$a_1\ a_2\ a_3\cdots\cdots a_n$〕が、偶（奇）順列のとき、$\alpha$を偶（奇）置換とよぶことにする。ここで任意の１個の偶順列において、その２数字の「入れ換え」をすると、それは奇順列となり、逆に奇順列における「入れ換え」により偶順列が得られるので、総順列の個数＝$n!$、偶順列の個数＝奇順列の個数＝$n!/2$、となることは明らかである。

さて、置換群論では順列の偶、奇が重要な意味を持つので、この「判定法」について考えることにする。先ず、〔１２３……〕の様に順序を正しく並ぶ順列を「正順」、〔２１３……〕の様に大小順が１個以上変動あるものを「乱順」とよぶことにする。正順な順列においては、数字の転倒（転置）数が０であるが、乱順な順列においては転倒数が偶、奇数のいずれかである。いま１、２、３、……、n、の任意の順列を〔$x_1\ x_2\ x_3\cdots\cdots x_n$〕とするとき、任意の$x_k$について、$x_k-x_i>0$（$k<i$）となるような$x_i$は、$x_k$に対する転倒を生んでいる。例えば順列〔２３１〕は、$2-1>0$、$3-1>0$より、１は２個の転倒をひき起こす。$2-3<0$、より２と３に関しては転倒

はない。この方法を基本としてx_1、x_2、……x_n、の差積（Δで示す）を定義する。

$$\begin{aligned}\Delta = &(x_1-x_2)(x_1-x_3)\cdots\cdots\cdots(x_1-x_n)\\ &\times(x_2-x_3)\cdots\cdots\cdots(x_2-x_n)\\ &\qquad\cdots\cdots\cdots\qquad\vdots\\ &\qquad\qquad\times(x_{n-1}-x_n)\end{aligned}$$

上のΔは、$k<i$、に対する(x_k-x_i)の積であるから、Δの正、負によって順列〔x_1x_2………x_n〕の偶、奇順列が決定する。この判定ソフトとその実行例が、Soft. 1 である。

Soft. 1

```
100 print "    置換の偶.奇,判定    "
110 input "文字数=";N
120 dim A(N):dim B(N):S=0
130 for I=1 to N : B(I)=0
140 input A(I) : next I
150 for I=1 to N
160 for J=I+1 to N
170 print A(I),A(J)
180 if A(I)-A(J)>0 then B(I)=B(I)+1
190 next : S=S+B(I) : next
200 print
210 print " 転置数=" S :print
220 for I=1 to N
230 print A(I);:next
240 if S mod 2=0 then 300 else 310
250 print
260 for I=1 to N
270 print A(I);:next
280 print print:print
290 print
300 print " ⇒ 偶順列です." : end
310 print " ⇒ 奇順列です."
320 goto 110
```

（例）

```
転置数=7
3 2 4 7 1 5 6 ⇒奇順列です.
転置数=18
3 1 5 10 2 9 6 8 7 4 ⇒偶順列です.
```

順列の概念は数学において必要であるばかりでなく、日常生活にも利用される場合が多い。これを基盤とするゲームも数多く登場した。「cubicの色合せ問題」は置換に関するゲームであったが、100年以上前にアメリカで考案された「15のコマ並べ」は純然たる「順列ゲーム」(6)であった。これはその後欧米各国で流行を極めたそうである。日本には明治の頃輸入されたといわれるが、子供の頃私もこれに熱中したことを覚えている。ゲームの内容は次のようである。

(1)　細い枠がある木の皿状の箱に、1より16までの番号を付したコマを並べ、16番のコマを除いて1個の空位を作る。（Fig. A）

Fig. A

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Fig. B

7	3	2	9
11		1	5
4	15	6	13
10	12	14	8

Fig. C

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

(2)　はじめの正順を崩して、任意の乱順とする。（乱順を作るときは、コマを取り出して移動してもよい。例えばこれらを、Fig. B、C、とする。）

(3)　ゲームの指示は、「1個の空位を利用してコマを上下、左右に移動しながら順列を補正し、乱順をFig. Aの正順に並べかえよ」ということである。ただし、空位は右の下方とする指示がある。

Fig. C、は1より13までは正順となり、15と14のみに転倒がある。ほとんど完成に近いが、14と15を正順にすると、以前の順列が崩れて失敗する。Fig. Bは更に困難である。これらを正順化することは、当時「懸賞問題」として提出されたそうである。このゲームの出発順列である1から15までの並べ方は15!で、1兆3000億を超える。これらの順列の正順化のために、どれ程多くの人が無駄な時間を費やしたことであろう。そこで以下Fig. B、C、のコマの正順化が可能であるか、不可能かの判定を順列論の立場から判定する。いま、最初に与えられた15のコマの第1列から15までの数を並べることにする。Fig. Bではそれは、7、3、2、9、11、1、5、4、15、6、13、10、12、14、8となる。この順列を前のSoft. 1で判定すると、転倒数が33となり奇順列となる。Fig. Cは明らかに14、15のみの転倒であるから転倒数が1となり奇順列である。Fig. Aは完全配列であるから転倒数が0で偶順列である。結論を述べると「ゲームの初期に与えられた15のコマの数の順列が奇順列であれ

ば、それを指定された方法で正順化は不可能である」ということになる。奇順列の正順化をどれ程時間を費やして試行してもラストに15、14が残りこれが解消できない悲鳴が聞こえるようである。奇順列の正順化不可能の証明は理論的に証明できるが、電算機では簡単に検証可能である。それは「1つの空所を利用して、コマを上下、左右に移動し転倒の個数を増減するとき、その個数の変化は偶数個である」という事実である。完全配列は転倒数0であるから、試行回数nを無限大としても、式表示すれば「(奇数)－(偶数)×n＝0」が不可能である。これが順列論から求められる懸賞問題の解答である。

(註)

本稿では順列の偶、奇を差積をもとにして判定した。しかし、置換を「互換の積」に分解し、その個数によっても判定できる。結果の数値に差異があり得るが、偶、奇は一意的に決定する。

§3　電算機による群表

3．1　群表について

われわれは日常の整数計算で、いわゆる「乗法九九表」を念頭において、暗黙的処理をする。これを群論計算におきかえたものが「群表」である。乗法九九は、被乗数、乗数をそれぞれ1より9までとするので、結果は9×9＝81、でおさまるが、群論の場合はこれで型がつかない。S(3)、S(4) ではそれぞれ36、576の結果が必要となる。更にS(5)では14400回の計算が必要である。なお整数乗法は$a\times b=b\times a$で、表は対角線に関して対称となるが、群論では$\alpha\beta=\beta\alpha$は不成立の場合もあり得るので、表の対称性は保証できない。しかし、この性質は群論におけるひとつの興味であり、表示された元素関係からも、群表は群の特性決定の要因を提示する。群表が群論のchartといわれる理由もここにある。

3．2　S(3) の群表

この場合元素は6個である。これらの中で偶置換に対応する行列は、Fig. 1、のように記号、≡を用いて1、2、3、に等置し、奇置換は1′、2′、3′、に等置した。なおこれらを具象化すれば、奇置換は「正3角形の3本の対称軸による、「裏がえし変換」であり、偶置換は重心を中心とする120度、240度、360度の「左回転変換であることがわかる (Fig. 1)。ここで「置換の結合 (積)」について例示する。ただし積の記号については、行列表現では(……) (……) の如く乗法記号を省略し、数字表現においては、$x\bigcirc y$、とし「○」を乗法記号とする。「1′○2≡2′」は次の意味をもつ、図の左端の3角形を (1 2 3) と表記すれば、これは変換1′により、3は固定して、1⇄2の変換が生じるので3角形は (2 1 3) となる、次の変換2 (120度の左回軸) で3角形は (3 2 1) となる。結果として3角形は (1 2 3)→(3 2 1) と変化されたことになるから、この変換が2′に対応している。なおこの群表では、縦書数字の変換xを被乗数、横書数字の変換yを乗数型とし、$x\bigcirc y$を記入した。以下もこの形式に従うものとする。

群表に表現する置換群S(n) の積の個数は、n＝3、n＝4、n＝5のとき、それぞれ36、576、14400である。表作成は前2者とするが、先ずそれらに共通する性質をのべる。第1は、偶置換×偶置換＝偶置換、である。これは表を作成してもすぐわかるが、具体的な操作からも理解できる。また、転置0も偶置換 (単位置換) として算定するので、偶置換全体の集合が群 (交代群)、A(n) をなすことが確認できる。第2は、表中の数字のダッシュをみてもわかるが、(偶(奇)、置換)× (奇(偶)、置換)＝奇置換となることである。nの種々の価により群S(n)は特有な性質を持つが、それらと代数系の関連は後節で考えることにする。S(3) の群表作成のソフトはSoft. 2、表はTable. 1である。

Fig. 1

偶置換 (1-3)

$1\equiv\begin{pmatrix}123\\123\end{pmatrix},\quad 2\equiv\begin{pmatrix}123\\231\end{pmatrix},\quad 3\equiv\begin{pmatrix}123\\312\end{pmatrix},$

奇置換 (1'-3')

$1'\equiv\begin{pmatrix}123\\213\end{pmatrix},\quad 2'\equiv\begin{pmatrix}123\\321\end{pmatrix},\quad 3'\equiv\begin{pmatrix}123\\132\end{pmatrix},$

置換の結合例 （正三角形の1垂線を軸とする裏返しと，120度左回転.）

$\begin{pmatrix}1&2&3\\\downarrow&&\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\&\downarrow&\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\\downarrow&&\\3&2&1\end{pmatrix}\Longrightarrow 1'\circ 2\equiv 2'$

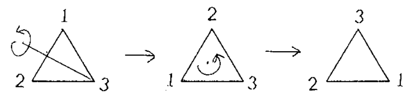


Table. 1

Table of Permutation Group S(3).

○	1	2	3	1'	2'	3'
1	1	2	3	1'	2'	3'
2	2	3	1	3'	1'	2'
3	3	1	2	2'	3'	1'
1'	1'	2'	3'	1	2	3
2'	2'	3'	1'	3	1	2
3'	3'	1'	2'	2	3	1

Soft. 2

```
100 dim B(6):dim A(6,3):dim U(36)
110 data 123,231,312,213,321,132
120 for I=1 to 6
130 read B(I) : print B(I) : next I
180 for I=1 to 6  : for J=1 to 3
200 print "A(";I;J;")=";:input A(I,J)
210 next  : next
230 X=0
240  for M=1 to 6  : for L=1 to 6
260 X=X+1
270 P(M,L)=A(L,A(M,1))*100+A(L,A(M,2))*10+A(L,A(M,3))
280 gosub 310
290 next : next
300 goto 340
310 for K=1 to 6
320 if P(M,L)=B(K) then U(X)=K
330 next K :return
340 print
350 print "   1     2     3     1'    2'    3'"
360 print "--------------------------------"
370 T=0
380 for X=1 to 36
390 T=T+1
400 if U(X)>3 then color 2  :print using "   ##'";U(X)-3;
410 if U(X)<=3 then color 7 :print using "   ## ";U(X);
420 if T mod 6=0 then print
430 if T=18 then print "
440 next X
```

3．3　S(4) の群表

この場合の元素は24個である。S(3)の場合と同様に偶置換に対応する行列は、Fig. 3－2、のように1、2、……、12、奇置換に対応する行列には1′、2′、……、12′、を等置した。なおこれらの具象化は前者と趣を異にし、正方形の対称軸による「裏がえし変換」、また「90度、180度、……、360度」の左回転変換、など個数が多い。(Fig. 2)

Fig. 2

偶置換(1-12)

$1 \equiv \begin{pmatrix}1234\\1234\end{pmatrix},\ 2 \equiv \begin{pmatrix}1234\\2143\end{pmatrix},\ 3 \equiv \begin{pmatrix}1234\\3412\end{pmatrix},\ 4 \equiv \begin{pmatrix}1234\\4321\end{pmatrix},\ 5 \equiv \begin{pmatrix}1234\\2314\end{pmatrix},\ 6 \equiv \begin{pmatrix}1234\\3124\end{pmatrix}$

$7 \equiv \begin{pmatrix}1234\\2431\end{pmatrix}\ 8 \equiv \begin{pmatrix}1234\\4132\end{pmatrix}\ 9 \equiv \begin{pmatrix}1234\\3241\end{pmatrix}\ 10 \equiv \begin{pmatrix}1234\\4213\end{pmatrix}\ 11 \equiv \begin{pmatrix}1234\\1342\end{pmatrix}\ 12 \equiv \begin{pmatrix}1234\\1423\end{pmatrix}$

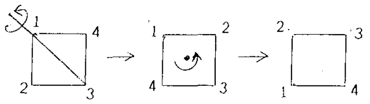
奇置換(1′-12′)

$1' \equiv \begin{pmatrix}1234\\2134\end{pmatrix},\ 2' \equiv \begin{pmatrix}1234\\3214\end{pmatrix},\ 3' \equiv \begin{pmatrix}1234\\4231\end{pmatrix},\ 4' \equiv \begin{pmatrix}1234\\1324\end{pmatrix},\ 5' \equiv \begin{pmatrix}1234\\1432\end{pmatrix},\ 6' \equiv \begin{pmatrix}1234\\1243\end{pmatrix}$

$7' \equiv \begin{pmatrix}1234\\2341\end{pmatrix}\ 8' \equiv \begin{pmatrix}1234\\2413\end{pmatrix},\ 9' \equiv \begin{pmatrix}1234\\3421\end{pmatrix},\ 10' \equiv \begin{pmatrix}1234\\3142\end{pmatrix},\ 11' \equiv \begin{pmatrix}1234\\4312\end{pmatrix},\ 12' \equiv \begin{pmatrix}1234\\4123\end{pmatrix}$

置換の結合例（正方形の対角線を軸とする裏返しと，90度左 回転）

$$\begin{pmatrix}1 & 2 & 3 & 4\\ \downarrow & & & \\ 1 & 4 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\\ \downarrow & & & \\ 2 & 3 & 4 & 1\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ \downarrow & & & \\ 2 & 1 & 4 & 3\end{pmatrix} \Longrightarrow 5' \circ 7' \equiv 2$$



行列表現の下図の変換表現では、最初は対角線1－3による裏がえしで、結果の正方形は1 4 3 2型となる。次回は90度左回転で、正方形は2 1 4 3型となる。つまり最初と終わりを比較して、1 2 3 4→2 1 4 3、となるから、対応行列2が得られる。以上が ⇨ 5′○7′≡2の意味である。他の場合にもこれに準じて結合する。

3．4　群表作成のプログラム

下位電算機ではコマンドも不十分であり、置換の問題を「文字関数」として扱うことは困難である。そこでプログラムでは、順列を構成する1、2、3、……等を分離した1桁の数字として入力し、個々の数字の変換結果を求めて、これを3、4桁の数字とすること、さらにこれらの数字と、もとの順列より得られる数字との異同を差別する、という初等的原則を採用した。4次置換表作成のための所要時間は50秒以内であり、プリントアウトには偶、奇置換などに、カラー表示がなされているので、表は美麗である。なお4次の場合、96個の数字の入力に時間を必要とするので、それらをA(*ijkl*)形式でDATAとして、先に電算機に読み込ませた、プログラムNo. 170～300がそれである。プログラムの実動はNo.310より始まる。

なお、上記プログラムの方式を拡張すれば、S(5)（正5角形の変換）の群表作成も可能である。しかし、電算機に120×120の画面は得られない。分割表の作成も有意義と思う。

Soft. 3

```
100 print "            Table of Permutation Group  S(4)."
110 print
120 dim A(24,4):dim B(255) :dim B(24) :dim H(25,25):dim P(24,24)
130 data 1234,2143,3412,4321,2314,3124,2431,4132,3241,4213,1342,1423
140 data 2134,3214,4231,1324,1432,1243,2341,2413,3421,3142,4312,4123
150 for I=1 to 24
160 read B(I): print B(I); : next
170 A(1,1)=1:A(1,2)=2:A(1,3)=3:A(1,4)=4:A(2,1)=2:A(2,2)=1:A(2,3)=4:A(2,4)=3
180 A(3,1)=3:A(3,2)=4:A(3,3)=1:A(3,4)=2:A(4,1)=4:A(4,2)=3:A(4,3)=2:A(4,4)=1
190 A(5,1)=2:A(5,2)=3:A(5,3)=1:A(5,4)=4:A(6,1)=3:A(6,2)=1:A(6,3)=2:A(6,4)=4
200 A(7,1)=2:A(7,2)=4:A(7,3)=3:A(7,4)=1:A(8,1)=4:A(8,2)=1:A(8,3)=3:A(8,4)=2
210 A(9,1)=3:A(9,2)=2:A(9,3)=4:A(9,4)=1
220 A(10,1)=4:A(10,2)=2:A(10,3)=1:A(10,4)=3:A(11,1)=1:A(11,2)=3
230 A(11,3)=4:A(11,4)=2:A(12,1)=1:A(12,2)=4:A(12,3)=2:A(12,4)=3
240 A(13,1)=2:A(13,2)=1:A(13,3)=3:A(13,4)=4:A(14,1)=3:A(14,2)=2:A(14,3)=1
250 A(14,4)=4:A(15,1)=4:A(15,2)=2:A(15,3)=3:A(15,4)=1:A(16,1)=1:A(16,2)=3
260 A(16,3)=2:A(16,4)=4:A(17,1)=1:A(17,2)=4:A(17,3)=3:A(17,4)=2
270 A(18,1)=1:A(18,2)=2:A(18,3)=4:A(18,4)=3:A(19,1)=2:A(19,2)=3:A(19,3)=4
280 A(19,4)=1:A(20,1)=2:A(20,2)=4:A(20,3)=1:A(20,4)=3:A(21,1)=3:A(21,2)=4
290 A(21,3)=2:A(21,4)=1:A(22,1)=3:A(22,2)=1:A(22,3)=4:A(22,4)=2:A(23,1)=4
300 A(23,2)=3:A(23,3)=1:A(23,4)=2:A(24,1)=4:A(24,2)=1:A(24,3)=2:A(24,4)=3
310 for M=1 to 24 : for L=1 to 24
320 P(M,L)=A(L,A(M,1))*1000+A(L,A(M,2))*100+A(L,A(M,3))*10+A(L,A(M,4))
330 gosub 350
340 next : next: goto 380
350 for K=1 to 24
360 if P(M,L)=B(K) then H(M,L)=K
370 next K : return : print
380 print "1 2 3 4 5 6 7 8 9 10 11 12 1' 2' 3' 4' 5' 6' 7' 8' 9'10'11'12'"
390 print "-----------------------------------------------------------------"
400 T=0
410 for M=1 to 24 : for L=1 to 24 : T=T+1
420 if H(M,L)<=12 then color 7 :print using "## ";H(M,L);
430 if H(M,L)>12 then color 2  :print using  ##'";H(M,L)-12;
440 if T mod 24=0 then print
450 if T=288 then print
460 next : next
470 color 7 : end
```

Table. 2

Table of Permutation Group S(4)

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

3．5　巡回群

群Gの任意の元αに対して、$\alpha^m=e$（単位元）となるような、最小正整数が存在する。このmを元αの位数という。例えば群$S(3)$において置換〔２３１〕は、１→２、２→３、３→１の順に置換する。つまりこれは120度の左回転であるから、３乗して恒等置換となる。一般に$\alpha^m=e$となるmを元αの位数とよんでいる。この結果$\{e, \alpha, \alpha^2, \cdots\cdots, \alpha^{m-1}\}$の元の集合は群をなす。この群を元$\alpha$によって生成される巡回群というが、特に置換群において、これは重要な役割をはたしている。

Soft. 4

```
100 print "  置換の位数計算      "
110 print
120 input "N=";N  :E=0
130 dim A(N):dim P(N*2,N*2)
140 for I=1 to N
150 print "A(";I;")="
160 input A(I) : next I
170 for I=1 to N
180 P(1,I)=A(I):next I
190 for I=1 to N
200 lprint A(I);:next
210 lprint "( 1 grade)"
220 for J=2 to N+3
230 for I=1 to N  : E=E+1
240 P(J,I)=A(P(J-1,I))
250 lprint P(J,I);
260 if E mod N=0 then lprint "(" J "grade)"
270 next : next
280 print "end"
```

実行例

```
6  4  2  1  7  5  3 ( 1 grade)
5  1  4  6  3  7  2 ( 2 grade)
7  6  1  5  2  3  4 ( 3 grade)
3  5  6  7  4  2  1 ( 4 grade)
2  7  5  3  1  4  6 ( 5 grade)
4  3  7  2  6  1  5 ( 6 grade)
1  2  3  4  5  6  7 ( 7 grade)
```

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

一般の置換の元について、その位数を求めることは非常に困難である。難題として提出されるものもある。これの解消のためSoft. 4を作成した。実行には、$S(n)$のnと、n個の置換の数字を入力するとよい。実行列は$n=7$で、置換の数字を〔６４２１７５３〕とした。これのべき乗が順次〔５１４６３７２〕、〔７６１５２３４〕、……、となりもとの置換の７乗が単位置換〔１２３４５６７〕にもどる。そこで最初の元をαとすると、$\alpha^7=e$（位数７）で$\{e, e^2, e^3, \cdots\cdots, e^6\}$が$S(7)$の７位の循環部分群となることがわかる。

3．6　正規部分群、商群、可解群

方程式の根の公式作成が、可能かどうかを決定するとき、重要となる諸群を定義する。

(1)　$G\supset H$とし、Gの任意の元aについて$aH=Ha$　$(aHa^{-1}=H)$となるとき、HをGの正規部分群という。

(2)　このとき、傍系aH、bH、……などについて、積 $(aH)(bH)=xH$となるxがGの元となり、逆元、単位元も決定するから、この傍系の集合は群をなす。これをGのHによる「商群」といい、G/Hとかく。G、Hそれぞれの位数をg、hとするとき、この商群の位数はg/hとなる。
　$(H=\{x, y, z, \cdots\cdots\}$ なら、$aH=\{ax, ay, az, \cdots\}$ の形となる。)

(3)　ひとつの群G_0があって、G_0の部分群G_iを続けてえらんで（例えば３個とする。）$G_0\supset G_1\supset G_2\supset G_3\supset E$（単位群）となったとき、商群の列（正規列）
G_0/G_1、G_1/G_2、G_2/G_3、G_3/E
がすべてアーベル群なら、群Gは可解群である、という。

§4 方程式の代数的解法と置換群

4．1 方程式の代数的解法

4次までの代数方程式の根の公式は存在する。しかし、5次以上の代数方程式の根の公式作成は不可能である。置換の解析によってこれを証明するのが以下の目的である。根の公式は方程式の係数相互の四則計算と、べき乗計算の合成によって根を求める手法の表示である。したがってこれを「代数的解法」とよんでいる。

3次方程式、4次方程式の根の発見者に関しては諸説があるが、その根の公式は、3次についてはCardano(1501－1576)の公式、4次はFerrari (1522－1565) の公式とよばれている。ところが5次及びそれ以上の次数の代数方程式の解法については、その後約300年間解決をみなかったが、これに明快な結論を与えたのが奇しくも同時代の天才青年数学者Galois (1811－1832) とAbel (1802－1829) であった。しかしそれは〝5次以上の次数の方程式は代数的に解くことはできない〟という否定的であっけない結論であった。

4．2 ガロア群とアーベル定理

いま数体kの元を係数とするn次方程式$f(x)=0$を考えると、根がn個存在する。これらをx_1、x_2、……、x_nとしてkに添加すると拡大体Kが得られる。ここでKの自己同型写像で、kの元を不変にする写像全体の集合が群をなす、これを方程式$f(x)$のガロア群という。例を実数を係数とする2次方程式$f(x)=0$にとると、この2根を共役複素数としα, $\bar{\alpha}$とおき、写像$\sigma(\alpha)=\bar{\alpha}$と定めると、基礎体$k$の元$a$については$\sigma(a)=\bar{a}=a$で不変となるから、$\sigma$は$k$を不変にするKの自己同型写像である。また明らかに単位写像eもこの条件をみたすので、$\{e, \sigma\}$がk－不変なKの自己同型写像の集合である。またここで$\sigma^2=e$となっているから、これは位数2の巡回群である。

さらに3次方程式$f(x)=0$の根をx_1、x_2、x_3とし、k、Kを前と同じように定義すれば、$f(x)$の係数が3根の対称式となるので、3根の置換がk－不変なKの自己同型写像となっている。この同型写像を、方程式$f(x)=0$のガロア群、とよんでいる。以上は次数が2、3次の場合であったが、n次の場合も成り立つので次の重要な結論が得られる。「方程式$f(x)$のガロア群は、n次の対称群S(n)である。」また方程式解法公式の演算方式から次の定理が得られる。

定理. 一つの方程式の根が代数的に求められるなら、その方程式のガロア群は可解群である。

これを受けてアーベルは決定的な定理を作った。つまり上定理の対偶命題より得られる次の定理がそれである。

〝5次以上の代数方程式は代数的に解けない〟

4．3 置換群解析による解法の判定

以上のガロア、アーベルの理論から、方程式解法公式作成の可、不可は、対称群A(n)が可解群であるかどうか、の判定によって決定されることがわかった。すでに知られることであるが2、3、4次方程式の根の公式作成の可能を確かめることにする。

(1) 2次方程式の場合。

以下S(n)、A(n)をS$_n$、A$_n$と略記すると、この場合のガロア群はS$_2$で正規列は、S$_2$⊃E(単位群)、となる。商群がS$_2$となり、S$_2$がアーベル群となるから2次方程式は可解である。

(2) 3次方程式の場合。

ガロア群はS$_3$で正規列は、S$_3$⊃A$_3$⊃E となり、商群列は、S$_3$/A$_3$、A$_3$/E、となる。ここで

$$S_3=\{1,\ 2,\ 3,\ 1',\ 2',\ 3',\}$$

$$A_3=\{1,\ 2,\ 3,\}$$ である、また

$$2A_3=\{2,\ 3,\ 1,\},\quad 3'A_3=\{3',\ 1',\ 2',\}$$

となることから $S_3=2A_3+3'A_3$ となる。2A$_3$、3$'$A$_3$は商群S$_3$/A$_3$の2元であり、

$$(2A_3)\ (3'A_3)=2\circ 3'A=2'A=\{2',\ 3',\ 1'\}$$

$$(3'A_3)\ (2A_3)=3'\circ 2A=1'A=\{3',\ 1',\ 2'\}$$

となるから、商群S$_3$/A$_3$がアーベル群、また

A_3/Eは明らかにアーベル群であるから、3次の対称群S_3は可解群となる。これが、3次方程式可解の理由である。

(3)　4次方程式の場合

ガロア群はS_4であるから正規列は

$S_4 \supset A_4 \supset B_4 \supset E$　となる。

ここでA_4は交代群、$B_4 = \{1, 2, 3, 4\}$である。ただし括弧内の数字は、群表における置換分類の番号とする。正規列のS_4、A_4、B_4の位数は24、12、4、1となるから、商群列S_4/A_4、A_4/B_4、B_4/Eの位数は2、3、4である。さて、S_4が可解群なることを証明するためには、上の3つの商群がいずれもアーベル群であることを示すとよい。

S_4/A_4は位数が2であるから、群表からもアーベル群であることがすぐわかる。またB_4/EはB_4である。群表でB_4の元1、2、3、4の結合表示数が、右下りの対角線に関して対称になっているから、$xy = yx$が成り立ちB_4はアーベル群である。次に商群A_4/B_4がアーベル群であることを示す。

$A_4 = \{1, 2, \cdots\cdots, 12\}$（偶置換）

$1B_4 = \{1, 2, 3, 4\}$

$5B_4 = \{5, 12, 8, 9\}$

$6B_4 = \{6, 10, 11, 7\}$　　ゆえに

$1B_4 + 5B_4 + 6B_4 = \{1, 2, 3, \cdots\cdots, 12\} = A_4$

ここで上の群がアーベル群であることを示すとよい。S_4の群表では、$5 \circ 6 = 6 \circ 5 = 1$である。

ゆえに　$(5B_4)(6B_4) = (6B_4)(5B_4)$　となり商群がアーベル群である。これよりS_4が可解群となり、4次方程の可解が証明できた。

(4)　5次以上の方程式の場合

この場合も従前の方法で証明可能であるが、群表が複雑になる。群表を利用する以前に、$S_5 \supset B_1 \supset B_2 \supset \cdots\cdots \supset E$、型の正規列が存在しないことを証明するのみで、$S_5$が可解群でないことがわかる。、また5より大きいnに対してもS_5が可解群でないから〝5次以上の次数の方程式は代数的に解くことはできない〟ことの証明が得られたことになる。

§5　おわりに

(1)　置換群研究で最も重要なことは、その元の分解性、可換性を知って「群表」を作成することである。その群の部分構造などは、この群の表を吟味すればすぐわかる。

(2)　S(3)、S(4) の群表作成のプログラムは、§3. で述べた。案外プログラムは、for～nextの簡単なloopにまとまった。これを手書計算で作成した表については、すでに発表したことがある。

(3)　電算機と相対したとき、基本的な関係は「自分はどう考えるか」と「電算機はどう考えるか」である。四則の基本演算については、すでに組み込まれたソフトがあるからら問題なく作動する。しかし代数系問題は例外である。そこで必要となるのが、代数系から電算機への翻訳（プログラム）である。本稿ではプログラムに適当なloopを設けると共に、if～then形式で場合分けを多くし電算機の論理的思考をサポートすることにした。これらの過程で「形式的な代数構造」の真の理解が可能となり、「計算機の思考形式」との間の接点が発見できると思われる。

(4)　デロス神殿の故事にはじまる作図不能問題(立方倍積、円積、任意の角の3等分問題)がある。いずれも昔人を悩まし続けた難問であったが、後世になりこれらが定木とコンパスでは「作図不可能」であることが証明された。「何故に不可能であるか？」の理由は、置換群の構造からわかる。方程式とも関連するのでこれを割愛する。

参考文献

(1)　Buchberger and others,: Computer Algebra. Springer-Verlag, Computing supplement 4, (1982).

(2)　Donald D,: Computer in number theory. Computer science press, (1982).

(3)　Jacobson,: Lectur in Abstract Algebra (3). Springer Verlag. (1964).

(4)　Jacobson D,: Topic in the Theory of Group permutations, London Mathematical Society

Lectur Note series. 42, Cambridge Univ. press, (1980).

(5) Senga and Tanimura,: On the structure of comutativity of permutation groups.Sci.Rep. Gifu uni.Natur.Sci. Vol.2. No.5, (1961).

(6) 数学小景.（高木貞治著）. 岩波書店.（1943）.

(7) ガロア理論.（エムポストニコフ著、日野寛三訳）. 東京図書.（1972）.

(8) ガロア理論入門.（寺田文行著）. 東京図書.（1980）.

(9) 神々の愛でし人.（レオポルド著、市井三郎訳）. 日本評論社.（1950）.