２６「ガロア補足」

前に書いた「ガロア」は、後で読み返してみると解りにくい。

“「群」という数学的構造と「体」という数学的構造の間を行ったり来たりすることで、数学的素性を明らかするという画期的な方法論”といってもどういうこと？と言われてしまいそうだ。

もう少し解りやすく書き直さなければならないと思っていたが、ガロア理論をわかりやすく説明するのはとても難しいと、しり込みしていた。

ガロア理論の出発点は代数方程式である。

１，２，３，４次方程式については四則演算（＋ －×÷）と冪根（べき根 $\sqrt{\ }$ $\sqrt[3]{\ }$ $\sqrt[4]{\ }$ ･･･）で解ける根の公式がある。

□２次方程式：９世紀ころ発見

$aX^2+bX+c=0$ の解の公式

$$X=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

□３次方程式：１６世紀半ば／イタリアのカルダーノ

$aX^3+bX^2+cX+d=0$ の解の公式

$$X_1=\sqrt[3]{-\frac{27c+2a^3-9ab}{54}+\sqrt{(\frac{27c+2a^3-9ab}{54})^2+(\frac{3b-a^2}{9})^3}}+\sqrt[3]{-(\frac{27c+2a^3-9ab}{54})-\sqrt{(\frac{27c+2a^3-9ab}{54})^2+(\frac{3b-a^2}{9})^3}}-\frac{1}{3}a \qquad \text{----------①}$$

これが１つの解。あと２つは、

$$\omega_1=1,\ \omega_2=\frac{-1+i\sqrt{3}}{2},\ \omega_3=\frac{-1-i\sqrt{3}}{2}$$ （ω_2，ω_3は１の三乗根、i は虚数単位で $i=\sqrt{-1}$ ）

として、X_1 の大きな３乗根の前に、ω_2とω_3 が交互につく。

つまり、$X_2=\omega_2\sqrt[3]{前}+\omega_3\sqrt[3]{後}-\frac{a}{3}$，$X_3=\omega_3\sqrt[3]{前}+\omega_2\sqrt[3]{後}-\frac{a}{3}$ である。

□４次方程式：１６世紀半ば／イタリアのフェラーリ

$aX^4+bX^3+cX^2+dX+e=0$　の解の公式

省略。

３次方程式が上記のようなのだから、４次はもっとずっと複雑な式である。しかし、四則演算と冪根だけで解ける解の公式は存在し必ず解ける。

一般にｎ次方程式は、ガウスの証明した代数学基本定理により、複素数の範囲内で必ずｎ個の解を持つ事がわかっている。従って５次方程式には５つの解が存在するわけである。

しかし、５次方程式については、４次までと異なり四則演算と冪根による解の公式がない。この事実を証明することをきっかけに発展したのがガロア理論なのである。

２次方程式　$aX^2+bX+c=0$　---------- ②

の２つの解をα，βとすると、$(X-\alpha)(X-\beta)=0$ となる。

これから、$X^2-(\alpha+\beta)X+\alpha\beta=0$ となるので、根と係数の関係は$a=-(\alpha+\beta)$，$b=\alpha\beta$ となっている。

これからわかるように、αとβ は入れ替えても全く変わらず対称性を持つ。

３次方程式　$aX^3+bX^2+cX+d=0$　---------- ③

の３つの解をα，β，γとすると、$(X-\alpha)(X-\beta)(X-\gamma)=0$

これから、$X^3-(\alpha+\beta+\gamma)X^2+(\alpha\beta+\beta\gamma+\gamma\alpha)X-\alpha\beta\gamma=0$

となるので、根と係数の関係は$a=-(\alpha+\beta+\gamma)$，$b=\alpha\beta+\beta\gamma+\gamma\alpha$，$c=-\alpha\beta\gamma$ となり、３次方程式についても、αとβとγ は入れ替えても全く変わらず対称性を持つことがわかる。

このことは４次方程式、、、でも同様である。

方程式の係数は、解の順番を置き換える操作に関して不変な性質を持っていることがわかる。

そこで、解の入れ替えによって作られる集合が、どのような性質を持つのかということが何か重要な意味を持つと考えられる。

解ける場合と解けない場合とでは何かが違うはずである。この、「解の入れ替え」という考え方が発展して「群」という数学的対象となった。群とはある集合の対称性をあぶり出す道具になる。

ある作用で不変に保たれる性質が対称性で、群を扱うことによってそれを数学の理論に乗せることができる。ガロアによって構築されたこの『群論』は、今では現代数学の中核の一つとなっている。

さて、ガロア理論の本質を知るためには、どうしても説明が必要になることがある。それは、「群」と「体」である。

「群」とは、、、「その範囲で自由に演算（足したり掛けたりなど）ができる集合」のことで、次の３つの条件を満たすものをいう。

集合Ｇの任意の２つの元(要素)x，ｙに対して、Ｇの中にx･ｙが含まれ一意(１対１)に定まり、

1. 結合法則が成り立つ：$x(yz)=(xy)z$ ‥‥繋ぐことができる性質
2. 単位元がある：Ｇに「e」と書かれる特定の元が存在して、Ｇの任意の元x に対して$xe=x$ が成り立つ ‥‥変えないことができる性質
3. 逆元がある：Ｇの任意の元x に対して$xx^{-1}=e$ をみたすＧの元「x^{-1}」がある‥‥もとに戻すことができる性質

以上の３つの条件をみたすとき集合Ｇは「群」であるという。

群の中でどうしても知らなければならない用語として、

『巡回群』→１つの要素を何回も繰り返して作られる群

『正規部分群』→ある群の部分群Ｈ（群の中に含まれる群）で、群の全ての元ｇに対して、

ｇＨｇ$^{-1}$＝Ｈがなりたつもの。

これは、Ｈに対し任意のｇを掛け（ｇという操作をおこない)、その結果にｇの逆元ｇ$^{-1}$を掛けると元に戻ることをいっている。

「体」とは、、、「数の集合で、その範囲で自由に四則演算ができる集合」のことである。

＋ －× ÷ の四則計算の答えが必ずその中に存在する、といえばわかりやすい。

例えば、自然数（0,1,2,3･･･）は体ではない。引き算と割り算の答えがその中に存在しない場合があるからである。

体の中でどうしても知らなければならない用語として、

『拡大体』→体にいろいろな数を追加して、さらに大きな体にすること。

例えば、有理数（整数［･･･−1,0,1,2,3･･･］，少数，分数）からなる集合は、四則演算の答えが必ずその中にあるので体であり、これを有理数体と呼ぶ。しかし、有理数体は冪根 $\sqrt{\ }$ $\sqrt[3]{\ }$ ･･･に対しては答えがその中にない。そんな時は、有理数体に無理数を付け加えて、実数体（有理数＋無理数の集合）を作ることができる。これは体の拡大したものなので拡大体と呼ぶ。さらに虚数（マイナス数の$\sqrt{\ }$ ）を付け加えて複素数体（有理数体＋無理数＋虚数の集合）とすれは、どのような演算に対しても、答えがその中にある体とすることができる。

『自己同型』→体の中の数を同じ体の中の他の数に対応させる場合で、次の３つの条件を満たすもの（体の中の数をもれなく、重複なく自分自身の体の数に対応させる）

ⅰ　２つの異なる数が同じ数に対応することはない

ⅱ　どの数に対しても必ずそれに対応する数が同じ体の中に存在する

ⅲ　ある関数ｆ（function）によって、四則計算は保存される

$x+y=z$ なら、$f(x)+f(y)=f(z)$，$f(x+y)=f(x)+f(y)$，$f(x\cdot y)=f(x)\cdot f(y)$

自己同型には２種類ある。有理数体Ｑ（整数，少数，分数の集合)の拡大体Ｑ(√2)、これはＱに無理数 $\sqrt{2}$ だけを追加した体で、$1+3\sqrt{2}$ や$-3-7\sqrt{2}$ など$a+b\sqrt{2}$ となるものを含む。

そうすると、１つは $f(x)=x$ となるもの（有理数体はすべて１対１に対応するので、このタイプの自己同型になる）もう１つは、$f(a+b\sqrt{2})=f(a-b\sqrt{2})$ となる（有理数部分を不変に保ち、無理数部分の符号が変わる）もの。拡大体$\mathrm{Q}(\sqrt{2})$ などが、このタイプの自己同型になる。これを共役といい、共役を２回行うと元に戻る。自己同型にはこの２種類しかない。

方程式の解のすべての入れ替えが作る集合は「群」である。この群の性質を突き詰めていくことで、その方程式に解の公式が存在するかどうかがわかる、というのがガロアの発想だ。

方程式の解は入れ替えに対して不変なので、その群の元は対称性をもつ。例えば３次方程式の場合でいうと、それは正三角形を「回転」と「裏返し」によって重ね合わせる操作に一致するため、それでわかりやすく説明できる。

３次方程式の解をα，β，γとすると、３つの解の入れ替えの作る集合は群とな

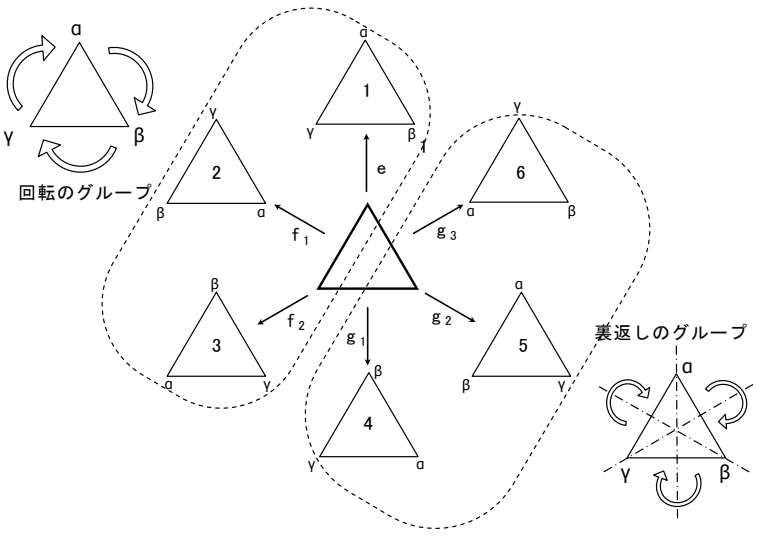

図1　3つの解の入れ替がつくる群

る。（図１参照）

３次方程式の解の入れ替えが作る群は 3!＝3×2×1＝6 個の元（下記 1～6）を持つ。

〔A〕中心点に対する回転

1　0°の回転 ------ 「e」単位元

2　120°の回転 ------「f_1」

3　240°の回転 ------ 「f_2」

〔B〕３本ある中心線に対する裏返し

4　30°軸に対する裏返し------ 「g_1」

5　90°軸に対する裏返し------ 「g_2」

6　150°軸に対する裏返 ------ 「g_3」

ガロアは解そのものではなく、「回転」「裏返し」など正三角形を重ね合わせる対称操作で示される、解の入れ替えが作る群について、その中の自己同型（三角形が重なり合う）全体の集合がつくる群に注目。この自己同型全体の集合を、ガロアの発見に尊敬の意味を込めて「ガロア群」と呼んでいる。

そしてガロア群の中に正規部分群があるかどうかが重要になる。この正規部分群は有理数の部分を不変に保つ操作に対応している。

この正規部分群が存在することこそ、方程式の解の公式に対するガロアの中心的アイデアなのである。

有理数体Q(整数，少数，分数の集合)に、３次方程式の解 $(\alpha,\ \beta,\ \gamma)$ のうちどれか１つ、例えば α（これは①式に示すようにいくつかの $\sqrt{\ }$ や $\sqrt[3]{\ }$ などを含む）と、１の３乗根に含まれるその要素 $(\sqrt{3},\ i)$ を加えた拡大体 $Q(\alpha,\ \sqrt{3},\ i)$ を作る。そしてその自己同型を考える。

１の３乗根は１のみではなく３つある。

前述した、 $\omega_1 = 1,\ \omega_2 = \dfrac{-1+i\sqrt{3}}{2},\ \omega_3 = \dfrac{-1-i\sqrt{3}}{2}$ $(\omega_3 = {\omega_2}^2)$である。

すると、この拡大体には残りの解 $\beta,\ \gamma$ が必ず含まれることになる。$\beta,\ \gamma$ は $\alpha,\ \sqrt{3},\ i$ を使って四則演算で表せる。その理由は、自己同型には有理数部分を不変に保ち、無理数部分の符号が変わるもの（共役）を含んでいるためである。

例えば、$\alpha = 2\omega_2 = 2\times\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right) = -1+i\sqrt{3}$ とすると、その共役 $-1-i\sqrt{3} = 2\omega_3$ は、必ず含まれる事になるのだ。これが「体」の概念の優れたところである。

このようにして作った拡大体 $Q(\alpha,\ \sqrt{3},\ i)$ の自己同型全体が作る群を考える。それは解の入れ替えすべてが含まれる群であり、３次方程式の場合でいえば正三角形の重ね合わせが作る群と同じになる。これがガロア群である。そして、このガロア群の中に正規部分群が存在することがポイントとなる。

正規部分群は、ちょうど公約数のようなものであり、この正規部分群で元の群を割っていくことにより、解の持つ対称性が確かめられることになる。

ここまでくれば、ｎ次方程式に四則演算と冪根による解の公式が存在するかどうかを判定する方法が

明らかにできる。それは次のような手順となる。

n 次方程式の解の入れ替えが作る群について、

1．その中の自己同型全体が作る群（ガロア群）を取り出す〔解がすべてこの群に含まれている〕

2．その群から、素数（2,3,5,7,11･･･）の元からなる正規部分群を取り出す〔解の入れ替えで式の値が変化しない群〕

3．正規部分群を取り出すときに、もとの群をその正規部分群で割った残りの群の元の数が素数で、かつ巡回群となっていること。〔有理数部分を不変に保つ共役の解が含まれる〕

4．1から3の操作で作っていった群が最終的に単位元「e」に達すること〔体の中にすべての解が含まれる〕　以上である。

3次方程式に当てはめると、3つの解の入れ替えの作る群を示した図1より、

a．元の数は6

b．正規部分群として、「e，f_1，f_2」「e，f_1，f_2，g_1，g_2，g_3」の2つ。この中で素数の元からなる正規部分群は、中心点に対する回転の作る群「e，f_1，f_2」である（図2参照）

c．もとの群を正規部分群で割った残りの群の元の数は、「e，f_1，f_2」のとき6÷3＝2で、図3に示す3つの群（巡回群）となり、さらにその群で割ると単位元「e」が残る。

正規部分群

○	e	f_1	f_2	g_1	g_2	g_3
e	e	f_1	f_2	g_1	g_2	g_3
f_1	f_1	f_2	e	g_2	g_3	g_1
f_2	f_2	e	f_1	g_3	g_1	g_2
g_1	g_1	g_3	g_2	e	f_2	f_1
g_2	g_2	g_1	g_3	f_1	e	f_2
g_3	g_3	g_2	g_1	f_2	f_1	e

図2　群の6つの元相互の演算と正規部分群

	e	g_1
e	e	g_1
g_1	g_1	e

	e	g_2
e	e	g_2
g_2	g_2	e

	e	g_3
e	e	g_3
g_3	g_3	e

図3　正規部分群を取り出した残りの群とその演算

正規部分群「e，f_1，f_2」は、正三角形の中心に対する回転が作る群であるが、それは1の3乗根であり図4に示すようにx軸を実数軸，y軸を虚数軸とする平面（複素平面）上で、120°，240°回転した位置の座標を示している。

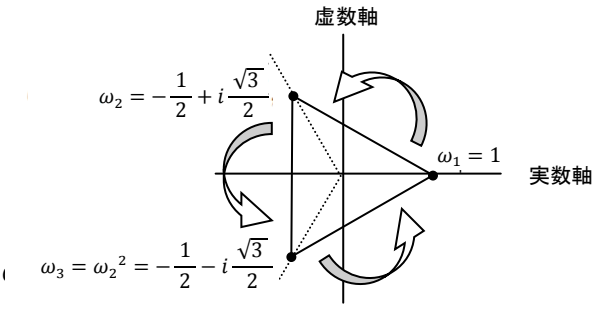

図4　複素平面上の正三角形の点

4次方程式の場合、

4次方程式の解の入れ替えが作る群（ガロア群）は 4!＝4×3×2×1＝24 の元となる。（これをS_4と表す）

3次方程式は正三角形の回転と裏返しで表せたが、4次方程式の場合ちょうど正六面体（立方体）の回転で表すことができる。（図5）

立方体を回転してもとの立方体に重ね合わせるやり方は全部で２４通りある。

〔A〕向かい合う面の中心を通る軸の周りの回転（面中心タイプ）

対向する面は３組あるので軸は３本、回転は 90°180°270°の３通りで３×３＝９通り

〔B〕対角線の周りの回転（対角線タイプ）

対角線は４本、それぞれの対角線に対して 120°240°の回転があるので４×２＝８通り

〔C〕向かい合う辺の中心を通る軸の周りの回転（辺中心タイプ）

対向する辺は６組あるので軸は６本、回転は 180°の１通りで６×１＝６通り

最後に全く動かさない恒等置換が１通りあるので、合計９＋８＋６＋１＝２４通りとなる。

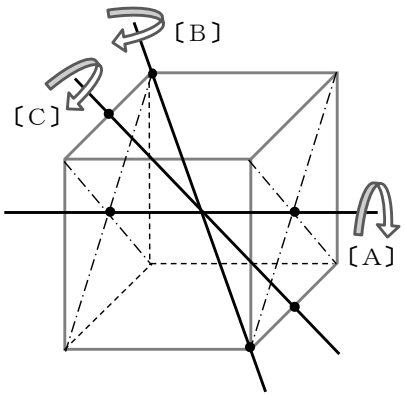

図5 正六面体の回転による自己同型

a. ２４通りの入れ替えについて、偶数置換（入れ替えを偶数回行うことでできる）と奇数置換に分ける。（４つの解の入れ替えが作る２４元による組み合わせ演算を末尾に示す。表は「１，２，３，４」の４つの数の入れ替えで示している）

偶数置換：合計１２

・面中心タイプの 180°回転 ‥‥‥３

・対角線タイプ ‥‥‥‥８

・恒等置換「e」 ‥‥‥‥１

奇数置換：合計１２

・面中心タイプの 90°270°回転‥‥６

・辺中心タイプ ‥‥‥‥６

偶数置換のみによって作られる群を交代群（A_4）という。A_4は正規部分群ではない。

b. A_4のうち、３つある面中心タイプの 180°回転に「e」を加えた４元からなる群は正規部分群となる。これをＮとする。

c. A_4をＮで割ると$A_4 \div N \rightarrow 12 \div 4 = 3$ となる。そして最終的には「e」が残る。

A_4が正規部分群でないにも拘わらず４次方程式が解けるのは、A_4には正規部分群Ｎが含まれ、さらに$A_4 \div N$が３つの元からなる、４組の正規部分群（対角線タイプを２つずつ組み合わせた４つの群）という特別な形をしているためである。

各段階における元の数を並べてみると、２４→１２→４→２→１となっている。

この元の数で割った残りの群の元の数は、２→３→２→２（24÷12＝2，12÷4＝3，4÷2＝2，2÷1＝2）である。

これが何を表すかというと、解の公式に現れる冪根と１対１に対応しているのである。つまり、４次方程式の解の公式は平方根３回と３乗根１回取る必要があることがわかる。

以上より、４次方程式は四則演算と冪根による解の公式があることが確められた。

最後に問題の５次方程式である。

５次方程式の解の入れ替えが作る群（ガロア群）は $5!=5\times4\times3\times2\times1=120$ の元となる。

３次方程式の正三角形，４次方程式の正六面体のように、１２０の元の入れ替えを直接表せる正多面体はない。しかし、１２０の元から偶数置換だけを取り出した残りの６０の元に対しては、正二十面体が対応する。この正二十面体のすべての置き換えのパターンは６０通りある。

５次方程式を解くことは、この６０通りの回転操作の中から素数の元を持つ巡回群を割り出して、正規部分群を見出すことが必要となる。

素数の元という条件から候補になるのは２，３，５である。

・２の場合、３０通りだけの操作を抜き出す、

・３の場合、２０通りだけの操作を抜き出す、

・５の場合、１２通りだけの操作を抜き出すことが必要だ。

大変な数のパターンになるのでこれ以上は割愛するが、やってみるといずれも当てはまる回転操作に対応する群は見出せない。結局正規部分群は見つけることはできないのである。

３つのもの，４つのものの入れ替えと、５つのものの入れ替えでは、対称性についての性質が基本的に異なるのである。

代数的手法（四則演算と冪根の演算）による、５次方程式の解の公式はないことがガロア理論により証明されたが、超絶的な手法による解の公式は得られている。

フランスの数学者エルミートは、楕円関数を用いて５次方程式の解の公式を導いている。楕円関数は、同じくフランスの数学者ヤコビの研究成果により発展したものである。

楕円の弧の長さを計算するときに出てくるのが楕円積分であるが、楕円関数はその逆関数である。楕円関数は三角関数と似た性質を持ち、加法定理や倍公式などがある。

エルミートは楕円関数の５倍公式を導き、工夫して変形した $X^5+X+c=0$ という、ブリンク・ジラード標準形の５次方程式について、解の公式を導いたのである。

（５次方程式の一般形、$aX^5+bX^4+cX^3+dX^2+eX+f=0$ から $X^5+X+c=0$ という形に導くのも相当の工夫が必要）

実は楕円関数による解法のアイデアは、ガロアの遺稿の中間部分に述べられている。ガロアはそこまで気付いていた。

ガロア理論の真髄は、体の拡大を群に結び付けてしまう点にある。体は無限集合であることが多く、その拡大体も無限集合なので、それらの計算は非常に難しい。

群は体より扱いやすいし計算もわかり易いので、群で考える方がやりやすい。群を調べることで体の性質を知ることができる。群は拡大体の構造を、分かりやすいように輪切りにして見せてくれる Ｘ線ＣＴのようなものといえるだろう。

若干２０歳のガロアの頭脳に生まれたアイデアが、今日の数学の発展に大きな影響を与えることになった。

しかし、このアイデアが現代に伝わったこと、そのことが奇跡に近いのだ。それを知るためには、ガロアの生涯について知る必要がある。

決闘の前日、夜を徹して遺稿となる論文を書きながら『もう時間がない！』というところを読むと、どうしても込み上げてきてしまうのは私一人ではないだろう。
（２０１１．９．２５）

「付－５」に、藤原正彦著「天才の栄光と挫折」からガロアの部分の抜粋を掲げる。

各群に対する乗算表

■4 つの数（1, 2, 3, 4）総ての入れ替え（ガロア群S_4）に対する乗算表（24×24=576 通り）

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		1234	**1243**	**1324**	**1432**	**1342**	**1423**	**2134**	**2143**	**2314**	**2341**	**2413**	**2431**	**3124**	**3142**	**3214**	**3241**	**3412**	**3421**	**4123**	**4132**	**4213**	**4231**	**4312**	**4321**
1	**1234**	1234	1243	1324	1432	1342	1423	2134	2143	2314	2341	2413	2431	3124	3142	3214	3241	3412	3421	4123	4132	4213	4231	4312	4321
2	**1243**	1243	1234	1342	1423	1324	1432	2143	2134	2341	2314	2431	2413	3142	3124	3241	3214	3421	3412	4132	4123	4231	4213	4321	4312
3	**1324**	1324	1423	1234	1342	1432	1243	2314	2413	2134	2431	2143	2341	3124	3142	3124	3421	3142	3241	4213	4312	4123	4321	4132	4231
4	**1432**	1432	1342	1423	1234	1243	1324	2431	2341	2413	2143	2314	2134	3421	3241	3412	3142	3214	3124	4321	4231	4312	4132	4213	4123
5	**1342**	1342	1432	1243	1324	1423	1234	2341	2431	2143	2413	2134	2314	3241	3421	3142	3412	3124	3214	4231	4321	4132	4312	4123	4213
6	**1423**	1423	1324	1432	1243	1234	1342	2413	2314	2431	2134	2341	2143	3412	3214	3421	3124	3241	3142	4312	4213	4321	4123	4231	4132
7	**2134**	2134	2143	3124	4132	3142	4123	1234	1243	3214	3241	4213	2431	3124	1342	2314	3241	4312	4321	1423	1432	2413	2431	3412	3421
8	**2143**	2143	2134	3142	4123	3124	4132	2143	2134	3241	3214	4231	4213	1342	1324	2341	2314	4321	4312	1432	1423	2431	2413	3421	3412
9	**2314**	2314	2413	3214	4312	3412	4213	1324	1423	3124	3421	4123	4321	1234	1432	2134	2431	4132	4231	1243	1342	2143	2341	3142	3241
10	**2341**	2341	2431	3421	4321	3421	4231	1342	1432	3142	3412	4132	4312	1243	1423	2143	2413	4123	4213	1234	1324	2134	2314	3124	3214
11	**2413**	2413	2314	3214	4213	3214	4312	1423	1324	3421	3124	4321	4123	1432	1234	2431	2134	4231	4132	1342	1243	2341	2143	3241	3142
12	**2431**	2431	2341	3241	4231	3241	4321	1432	1342	3412	3142	4312	4132	1423	1243	2413	2143	4213	4123	1324	1234	2314	2134	3214	3124
13	**3124**	3124	4123	4132	3142	4132	2143	3214	4213	1234	4231	1243	3241	2314	4312	1324	4321	1342	2341	2413	3412	1423	3421	1432	2431
14	**3142**	3142	4132	4123	3124	4123	2134	3241	4231	1243	4213	1234	3214	2341	4321	1342	4312	1324	2314	2431	3421	1432	3412	1423	2413
15	**3214**	3214	4213	2314	3412	4312	2413	3124	4123	1324	4321	1423	3421	2134	4132	1234	4231	1432	2431	2143	3142	1243	3241	1342	2341
16	**3241**	3241	4231	4321	3421	4321	2431	3142	4132	1342	4312	1432	3412	2143	4123	1243	4213	1423	2413	2134	3124	1234	3214	1324	2314
17	**3412**	3412	4312	4213	3214	4213	2314	3421	4321	1423	4123	1324	3124	2431	4231	1432	4132	1234	2134	2341	3241	1342	3142	1243	2143
18	**3421**	3421	4321	4231	3241	4231	2341	3412	4312	1432	4132	1342	3142	2413	4213	1423	4123	1243	2143	2314	3214	1324	3124	1234	2134
19	**4123**	4123	3124	2134	2143	2134	3142	4213	3214	4231	1234	3241	1243	4312	2314	4321	1324	2341	1342	3412	2413	3421	1423	2431	1432
20	**4132**	4132	3142	2143	2134	2143	3124	4231	3241	4213	1243	3214	1234	4321	2341	4312	1342	2314	1324	3421	2431	3412	1432	2413	1423
21	**4213**	4213	3214	2314	2413	2314	3412	4123	3124	4321	1324	3421	1423	4132	2134	4231	1234	2431	1432	3142	2143	3241	1243	2341	1342
22	**4231**	4231	3241	4321	2431	2341	3421	4132	3142	4312	1342	3412	1432	4123	2143	4213	1243	2413	1423	3124	2134	3214	1234	2314	1324
23	**4312**	4312	3412	2413	2314	2413	3214	4321	3421	4123	1423	3124	1324	4231	2431	4132	1432	2134	1234	3241	2341	3142	1342	2143	1243
24	**4321**	4321	3421	2431	2341	2431	3241	4312	3412	4132	1432	3142	1342	4213	2413	4123	1423	2143	1243	3214	2314	3124	1324	2134	1234

■交代群（A_4）に対する乗算表

		1	5	6	8	9	12	13	16	17	20	21	24	
		1234	**1342**	**1423**	**2143**	**2314**	**2431**	**3124**	**3241**	**3412**	**4132**	**4213**	**4321**	
1	**1234**	1234	1342	1423	2143	2314	2431	3124	3241	3412	4132	4213	4321	不変
5	**1342**	1342	1423	1234	2431	2143	2314	3241	3412	3124	4321	4132	4213	2番目→4番目に、3番目→2番目に、4番目→3番目に
6	**1423**	1423	1234	1342	2314	2431	2143	3412	3124	3241	4213	4321	4132	2番目→3番目に、3番目→4番目に、4番目→2番目に
8	**2143**	2143	3124	4132	2134	3241	4213	1342	2314	4321	1423	2431	3412	1番目と2番目,3番目と4番目を入れ替え
9	**2314**	2314	3412	4213	1423	3124	4321	1234	2431	4132	1342	2143	3241	1番目→3番目に、2番目→1番目に、3番目→2番目に
12	**2431**	2431	3241	4321	1342	3412	4132	1423	2143	4213	1234	2314	3124	1番目→4番目に、2番目→1番目に、4番目→2番目に
13	**3124**	3124	4132	2143	4213	1234	3241	2314	4321	1342	3412	1423	2431	1番目→2番目に、2番目→3番目に、3番目→1番目に
16	**3241**	3241	4321	2431	4132	1342	3412	2143	4213	1423	3124	1234	2314	1番目→4番目に、3番目→1番目に,4番目→3番目に
17	**3412**	3412	4213	2314	4321	1423	3124	2431	4132	1234	3241	1342	2143	1番目と3番目,2番目と4番目を入れ替え
20	**4132**	4132	2143	3124	3241	4213	1234	4321	1342	2314	2431	3412	1423	1番目→2番目に、2番目→4番目に,4番目→1番目に
21	**4213**	4213	2314	3412	3124	4321	1423	4132	1234	2431	2143	3241	1342	1番目→3番目に、3番目→4番目に,4番目→1番目に
24	**4321**	4321	2431	3241	3412	4132	1342	4213	1423	2143	2314	3124	1234	1番目と4番目,2番目と3番目を入れ替え

・8,17,24 は面中心タイプ(180° 回転) 、残りは対角線タイプ

・□は対角線どうしが一致しているもの（$gHg^{-1}=H$が成り立つもの）

■正規部分群（N）に対する乗算表

		1	8	17	24
		1234	**2143**	**3412**	**4321**
1	**1234**	1234	2143	3412	4321
8	**2143**	2143	2134	4321	3412
17	**3412**	3412	4321	1234	2143
24	**4321**	4321	3412	2143	1234

・面中心タイプ(180° 回転)と「e」からなる群

■対称群（A_4）から正規部分群（N）を除いた残り（４つの正規部分群）

		1	5	6
		1234	**1342**	**1423**
1	**1234**	1234	1342	1423
5	**1342**	1342	1423	1234
6	**1423**	1423	1234	1342

		1	9	13
		1234	**2314**	**3124**
1	**1234**	1234	2314	3124
9	**2314**	2314	3124	1234
13	**3124**	3124	1234	2314

		1	12	20
		1234	**2431**	**4132**
1	**1234**	1234	2431	4132
12	**2431**	2431	4132	1234
20	**4132**	4132	1234	2431

		1	16	21
		1234	**3241**	**4213**
1	**1234**	1234	3241	4213
16	**3241**	3241	4213	1234
21	**4213**	4213	1234	3241

■ガロア群S_4から対称群A_4を除いた残り（６つの単純群）

		1	2
		1234	**1243**
1	**1234**	1234	1243
2	**1243**	1243	1234

		1	3
		1234	**1324**
1	**1234**	1234	1324
3	**1324**	1324	1234

		1	4
		1234	**1432**
1	**1234**	1234	1432
4	**1432**	1432	1234

		1	7
		1234	**2134**
1	**1234**	1234	2134
7	**2134**	2134	1234

		1	15
		1234	**3214**
1	**1234**	1234	3214
15	**3214**	3214	1234

		1	22
		1234	**4231**
1	**1234**	1234	4231
22	**4231**	4231	1234