アーベル･ルフィニの定理

１．「アーベル・ルフィニの定理」とは，

「五次以上の代数方程式は、一般には、それを累乗根によって解くことが不可能である」

というものである．

以下，これについての解説と「ゆるやかな証明」[1] を述べるが，数学の知識の前提としては，高校二年程度のレベルを想定する．

２．与えられた方程式の次数をn≧1 とし、

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0 \qquad \cdots\cdots ①$$

とする．

方程式を「累乗根によって解く」とは，与えられた方程式の係数に加減乗除(四則)や累乗根を施すことでxの値を求めることをいうのであるが，およそ計算において四則は当たり前のことなので，加えて「累乗根を求める」ことによって解くことをこう呼ぶのである．四則のみで解かれる方程式は一次方程式のみで，それ以上の次数を持つ方程式は必ず累乗根によらなければ（一般には）解けないこともその理由である．

最初に，方程式に関するひとつの重要な定理について述べる．それは，すべての方程式には必ず解が存在することを保証するものである．[2]

[定理 1]「**複素係数のn次方程式は，複素数の範囲に少なくとも１個の解を持つ**」(ガウス)

というのがそれで，歴史的には「代数学の基本定理」と呼ばれてきたものである．

この定理は，ここでは証明なしで用いることにする．

この基本定理のおかげで，方程式①にはn個の解があることが保障されるのである．すなわち，方程式①は，定理１によって$x = x_1$を解に持つから，式$x - x_1$で割り切れる．その商は新たな「$x-1$次方程式」になる．ゆえに定理１によってこの方程式も解$x = x_2$を持つ．…以下　繰り返していけば，結局①はn個の解をもつ．このn個の解を，

$$x_1,\ x_2,\ \cdots,\ x_n$$

とすると，方程式①は，

$$(x-x_1)(x-x_2)\cdots(x-x_n) = 0$$

のように一次式の積に因数分解される．

ここではこれらの解を，累乗根によって解くためにどのような考え方をすればよいかを見ていく．

---

[1] 「ゆるやかな証明」とは，厳密でなく，とにかく理解することを目的とする説明のこと．

[2] もちろん，$0 \cdot x = 3$のようなものは除いて考えるものとする．

３．次に，$X^n = A$（A は定数)という形の方程式について述べる．このような方程式を「二項方程式」という．これを解くことがまさに「累乗根」なのであるが，これについては特別な扱いをする．

まず，もっとも簡単な二項方程式として$x^n = 1$を考える．[定理１]によってこの方程式にもn個の(複素数の)解が存在する．高校数学で習う**ド・モアブルの定理**を用いて，

$$x = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \quad （k \text{ は任意の整数}）$$

となるが，このとき，kによってはnと約分でき，n乗しなくても 1 になる場合がある．[3] そこであえてkとnが互いに素のときを，「1 の原始n乗根」と呼ぶ．特に$k=1$のときをξ （ギリシア文字のクシー）で表せば，

$$\xi = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

である．ξ は１の原始n乗根である．

これにより$x^n = 1$のすべての解は，$\xi, \xi^2, \xi^3 \cdots, \xi^n = 1$ で表される．これらはn個あって互いに異なる． ちなみに，$(\xi^k)^n$ （$1 \le k \le n-1$）を計算すれば，

$$(\xi^k)^n = (\xi^n)^k = 1^k = 1.$$

これらの解は，xy座標平面のx軸を実数軸に，y軸を虚数軸に取った**複素数平面**上では，半径 1 の円周上をn等分した分点の示す複素数になるという，非常に美しい性質を持つ．

$n=3$のとき，つまり，$x^3 = 1$の解である１の原始三乗根を，特にω（ギリシア文字のオメガ）で表すことがある．すなわち，

$$\omega = \frac{-1+\sqrt{-3}}{2}, \text{ または } \frac{-1-\sqrt{-3}}{2}$$

であるが，どちらか一方をωとすれば，もうひとつはω^2で表されるのが大きな特徴である．

一般の二項方程式$x^n = a$については，これも[定理１]によってn個の解が存在するが，そのどれか１つを$\sqrt[n]{a}$(一般には複素数)であらわせば，すべての解は，これに順次 1 の原始n乗根を掛けて作った数；

$$x = \sqrt[n]{a},\ \xi\sqrt[n]{a},\ \xi^2\sqrt[n]{a},\ \xi^3\sqrt[n]{a},\ \cdots,\ \xi^{n-1}\sqrt[n]{a}$$

で表される．これらの解も，複素数平面上では，半径$|a|$の円周上をn等分した分点の示す複素数となる($|a|$ は複素数平面での点aと原点との距離を表す).

以上が「累乗根」の意味である．従って，方程式の「累乗根による解法」とは，方程式の係数に対して四則を行なうことと，$X^n = A$という二項方程式を解くことを有限回繰り返すことによってすべての解を求めることをいう．

ただ，「一般的に解く」ためには，どんな方程式に対しても通用する「一般的な解法」すなわち「公式」が必要だが，そういうものは五次以上の方程式には存在しないといっているのが「アーベル・ルフィニの定理」なのである．

---

[3] 例えば，$n=6$ ならば，$k=2$のとき，$x = \cos\frac{4\pi}{6} + i\sin\frac{4\pi}{6} = \cos\frac{2\pi}{3} + i\cos\frac{2\pi}{3}$ で，これは３乗するだけで１になる．

では，どんなに工夫しても一般的解法が見つけられないことをどのようにして証明するのか.

n次方程式で$n \geq 2$の場合には，一般には累乗根を求めなくてはならないが，これがたまたま四則によって求められることもある．$x^2-5x+6=0$などは，$(x-2)(x-3)=0$と因数分解されてx＝２,３が得られるが，この解法は，与えられた係数の間の特別な関係（足して５，掛けて６になる２つの整数が２と３である）によるものであり，整数解であることを知りながら解いているのである．こうした「解法」は当然「一般的な解法」とはいえない．累乗根(この場合は平方根)が四則によって簡単に求められる場合は，ここでは問題ではない．しかし，$x^2-5x+5=0$などになるともうこの方法では解けない．解は明らかに整数や分数ではない．[4]　つまり整数である係数の四則の結果からは得られないものである.そこで最初に方程式の係数から四則計算によって得られるすべての値の集合を考え，その中に解があるか，ないかを考える･･･という思想が生まれた.

それが，「体(たい)」(数体，有利区域とも言う)という概念である．体とは，四則が保証された集合のことで，その中ではどの要素と要素の加減乗除にもその答えが同じ集合の中にある(ただし 0 での除算は除く)．だから自然数全体の集合 N や，整数全体の集合 Z は体ではないが，分数(有理数)全体の集合 Q は体である．数によって作られる体のなかでは，Q は一番「小さい」体といえる．Q を「有理数体」と呼ぶ．また，実数全体の集合 R，複素数全体の集合 C ももちろん体である． それぞれを「実数体」,「複素数体」と呼ぶ.

体は，広くとればいいというものではない．複素数体 C にはどんな方程式の解も含まれているが広すぎて役に立たない．ある人を探すのに，地球上には必ずいるという保証はいるが，それだけではその人を見つけられない．その人の行動範囲を特定し，そこにいなければさらに範囲を広げていくという方法を取らなければならない.

体によって方程式の「累乗根による解法」を言い表してみよう.

方程式①の係数$a_1, a_2, \cdots, a_n$から作られる体を K とする．これを基礎体(あるいは係数体)という．もし係数がすべて整数または有理数ならば，K は有理数体 Q となる．方程式の解がひとつでも K の中に存在するとき，この方程式は「K 上可約である」という．いいかえれば，この方程式は K の数を係数として因数分解できる.上述の$x^2-5x+6=0$などがその例である.しかし,たとえば$x^2-2=0$の解は K には存在しない($\sqrt{2}$は有理数ではない)．この場合は，「K 上既約である」という．いいかえれば、この方程式は K の数を係数として因数分解できない，あるいは，四則のみでは解けないのである．[5]

方程式①が四則のみで解けない場合には，基礎体 K の中のある数の累乗根を付け加えて，改めて四則を行った時のすべての値からなる新しい体を作る．このことを体の「拡大」といい，できた体を K の「拡大体」という（拡大された体から，もとの体を見たときには，これを「部分体」という）.

例えば，$x^2-5x+5=0$の基礎体は有理数体 Q であるが，解は$x=(5\pm\sqrt{5})/2$である．この解を構成する数の中で有理数でないのは$\sqrt{5}$という「累乗根」である．そこで Q に$\sqrt{5}$を付け加えた体を生成する．これを Q($\sqrt{5}$)と表す.

---

[4] $x^2-5x+5=0$の解を有理数とすれば，$x=b/a$(aは自然数，bは整数)とおいて代入すると，
$(b/a)^2-5b/a+5=0$より，$(b-(5/2)a)^2=(5/4)a^2$から　$b-(5/2)a=\left(\pm\sqrt{5}/2\right)|a|$となって，左辺は分数，右辺は無理数で矛盾する.

[5] 2 乗していくらでも 2 に近い数を四則によって求めることはできるが、ちょうど 2 になる数を有限回で求めることはできない．そこで「累乗根による解法」が必要になる.

$\mathrm{Q}(\sqrt{5})$は，集合としてみれば，有理数(分数)と$\sqrt{5}$を加減乗除して作られる数全体の集合だから，結局，$a+b\sqrt{5}(a,b$は有理数$)$という形の数全体となる．$\sqrt{5}$が何度も累乗されることがあっても結局必要な累乗根は$\sqrt{5}$だけでよい．$x^2-5x+5=0$は，この体の中にすべての解を持ち，従って，$\mathrm{Q}(\sqrt{5})$上で可約となり，

$$\left(x-\frac{5+\sqrt{5}}{2}\right)\left(x-\frac{5-\sqrt{5}}{2}\right)=0$$

のように一次式に分解できる．このことから$\mathrm{Q}(\sqrt{5})$を，方程式$x^2-5x+5=0$ の「分解体」という．[6]

複素数体 C はすべての方程式の分解体であるから，おのおのの方程式にとっては，分解体の存在が問題なのではなくて，基礎体の拡大によって分解体を構成することに問題の意味がある．

以上から，方程式①が累乗根で解けるならば，方程式①の係数体 K に適当な K の数r_1 からそのl_1乗根$\sqrt[l_1]{r_1}$ を追加して体 K'＝K($\sqrt[l_1]{r_1}$)を作り，さらに K'の中の数r_2 を選び，そのl_2乗根$\sqrt[l_2]{r_1}$ を追加して K"＝K'($\sqrt[l_2]{r_1}$)を作る…，こうして有限回ののち，方程式の解がすべて含まれている体，すなわち分解体を生成することができるはずである．しかし，このようにしても分解体を作ることができないならば，この方程式は累乗根で解けないことになるのである･･･．

「アーベル・ルフィニの定理」は，五次以上の代数方程式が累乗根で解けると仮定したときに，そこで生成された分解体に矛盾が起こることを導き，それが不可能であることを示すものである．

三次や四次の方程式が近世に解かれて以来，長く五次方程式が解かれないまま数世紀が経ち，次第に数学者たちには，どうも五次方程式にはそういった解法が存在しないのではないかという疑惑が生まれた．体の思想が生み出されたのは，そういう背景からであり，どうやっても解けないからこそ，その解けない理由を見つけるために考え出されたものだったのである．

４．次に，実際に，方程式を解くことと係数体の拡大との関係を見てみよう．簡単のため二次方程式を例に取る．二次方程式 $x^2+ax+b=0$ の係数体は簡単のため有理数体 Q とする．

一般的解法：b を右辺に移行し，両辺に$\left(\frac{a}{2}\right)^2$ を加えると，左辺は$(\quad)^2$の形に因数分解できる．

$$x^2+ax+\left(\frac{a}{2}\right)^2=-b+\left(\frac{a}{2}\right)^2$$

$$\left(x+\frac{a}{2}\right)^2=\frac{a^2-4b}{4}$$

ここで両辺の平方根をとれば，

$$x+\frac{a}{2}=\pm\frac{\sqrt{a^2-4b}}{2}$$

よって，求めるxは，

---

[6] ちなみに，$x^2-(3+\sqrt{5})x+3\sqrt{5}=0$という方程式があるとき，その基礎体は Q ではなく，Q（$\sqrt{5}$）であるから，この場合は基礎体を拡大する必要はないわけである．この方程式は基礎体上で可約である．

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

となる．中学でお馴染みの「解の公式」である．

この公式中の$\sqrt{a^2-4b}$という数が有理数ではない場合，基礎体 Q はこの方程式の分解体ではない．しかしこれを付け加えた体 Q($\sqrt{a^2-4b}$)を作れば，これは分解体になる．

そこで，この「付け加える数」の性質を調べよう．そのためには次数に関係なく表れる方程式の重要な性質を知らなければならない．それは「解と係数の関係」である．

例えば，二次方程式；

$$x^2+ax+b=0 \qquad \cdots\cdots③$$

の解をx_1，x_2とすれば，

$$x_1+x_2=-a \ ,$$

$$x_1x_2=c \qquad \cdots\cdots④$$

というものである．これは中学３年か高校１年あたりで習うのでよく知られているが，一般のn次方程式でも成り立つのである．三次方程式でいうと，

$$x^3+ax^2+bx+c=0 \qquad \cdots\cdots ⑤$$

の解をx_1，x_2，x_3とすると，

$$x_1+x_2+x_3=-a \ ,$$

$$x_1x_2+x_2x_3+x_3x_1=b \ ,$$

$$x_1x_2x_3=-c \qquad \cdots\cdots ⑥$$

となる．これは三次方程式の解と係数の関係である．さらに四次方程式；

$$x^4+ax^3+bx^2+cx+d=0 \qquad \cdots\cdots ⑦$$

では，やや複雑になるが，

$$x_1+x_2+x_3+x_4=-a \ ,$$

$$x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4=b \ ,$$

$$x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4=-c \ ,$$

$$x_1x_2x_3x_4=d$$

となる．もちろん４つの解はx_1，x_2，x_3，x_4 である．

明らかに美しい規則性が見てとれるが，この関係を一般的に言い表すために，方程式①を再掲する．

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n=0 \qquad \cdots\cdots ①$$

すると，n次方程式の「解と係数の関係」は，次のように言うことができる．

「n次方程式 ① のn個の解を，x_1，x_2，…，x_nとするとき，まず，すべての和は $-a$，次にn個の中から 2 個ずつ取ったものの積の和は a_2，さらに３個ずつ取ったものの積の和は $-a_3$，

… ，最後にn個すべての積は $(-1)^n a_n$ である.」

当然，このことは一般の自然数nについて証明しなければならないのであるが，取り合えずここでは証明抜きで認めることにしよう.

ここで「対称式」,「基本対称式」について説明する.

まず,「対称式」とは,「**若干個の文字からなる式があるとき，その中のどの文字どうしを入れ替えたとしても，また元の式と同じものになるとき，この式を対称式という**」.

さらに「基本対称式」とは,「**n個の文字があるとき，まずすべての文字の和からなる式，次にn個の中から2個ずつ取ったものの積の和，さらに3個ずつ取ったものの積の和，･･･，最後にn個すべての積からなる式の一組を基本対称式という**」.

こうして方程式①の解と係数の関係は，次の定理にまとめることができる.

[定理２] **方程式①の係数は，解の基本対称式で表される.**

そもそもなぜ「解と係数の関係」に「基本対称式」が現れるのかを簡単に見てみよう.

例えば，2 と 3 が解になるような二次方程式を作ってみよう．このとき次のようにするとよい.

$$(x-2)(x-3)=0$$

この方程式の解が 2 と 3 になることは理解できることと思うが，これを展開してみると,

$$x^2-5x+6=0$$

となって，$2+3=-(-5),\quad 2\times 3=6$ となっている．三次方程式でも，2 と 3 と 4 を解とする場合は,

$$(x-2)(x-3)(x-4)=0$$

を展開して,

$$x^3-9x^2+26x-24=0$$

とすると,

$$2+3+4=-(-9),\quad 2\times 3+3\times 4+4\times 2=26,\quad 2\times 3\times 4=-(-24)$$

となる．つまり，xとそれぞれの解との，差の積を作って，それを展開すれば,（x^n以外の）各項の係数は解の基本対称式になるのである.

これには，なぜ，ということはできない．強いていえば人間の作った式の美しさということになるのかも知れない.

対称式にはさらに著しい性質として,

[定理３]**あらゆる対称式は，同じ文字からなる基本対称式で表される.**

というのがある．これは「**対称式に関する基本定理**」と言われている．例えば，x,yについての対称式x^2+xy+y^2というのを，その基本対称式$x+y,xy$で表せば,

$$x^2+xy+y^2=x^2+2xy+y^2-xy=(x+y)^2-xy$$

となる．あらゆる対称式についてこのことが言えるのである（この定理も証明抜きで使用する）.

方程式の「解と係数の関係」はとても意味深いものである．それは次のことをあらわしている．すなわち，方程式の係数が，解の基本対称式で表されるとは，言い換えれば「基礎体のすべての数は，解の基本対称式で表される」ということである．基礎体のどの数も，係数どうしの四則計算から作る

ことができ，[7] そして係数は解の基本対称式で表されるからである．

対称式の一番の特徴は，その中の文字どうしの入れ替えによって変わらないことである．このことを「式の対称性」と呼ぶならば，この対称性こそが方程式の(累乗根による解法の)不可能性を生み出していくのである．

５．ここで，もう一度，先ほどの二次方程式の解法の中から現れてきた$\sqrt{a^2-4b}$を，今述べたことに基づいて解の基本対称式で表してみよう．

$x^2+ax+b=0$より，$a=-(x_1+x_2)$，$b=x_1x_2$ であるから，

$$\sqrt{a^2-4b}=\sqrt{(-(x_1+x_2))^2-4x_1x_2}=\sqrt{x_1{}^2+2x_1x_2+x_2^2-4x_zx_2}$$

$$=\sqrt{(x_1-x_2)^2}=|x_1-x_2|$$

絶対値の記号が出てきたが，これには本質的な意味はない．仮に，$x_1>x_2$なら$\sqrt{a^2-4b}=x_1-x_2$とすればよい．要は，根号が取れて，解による整式（正しくは「x_1，x_2による有理式」）になったことである．

ついでにx_1，x_2もそれぞれを解の対称式（と$\sqrt{a^2-4b}$）で表せば，$x_1>x_2$より，

$$x_1=\frac{-a+\sqrt{a^2-4b}}{2}=\frac{x_1+x_2+(x_1-x_2)}{2}=\frac{2x_1}{2}=x_1$$

$$x_2=\frac{-a-\sqrt{a^2-4b}}{2}=\frac{x_1+x_2-(x_1-x_2)}{2}=\frac{2x_2}{2}=x_2$$

となって，結局単なる恒等式になってしまうことは当然である．

以上のことをよく考えてみよう．

二次方程式 $x^2+ax+b=0$ の基礎体を有理数体としたとき，もし解x_1，x_2が有理数ならば，x_1-x_2も有理数である．

$\sqrt{a^2-4b}$が有理数でないときには，x_1-x_2も有理数ではないから，基礎体 Q を拡大しなくてはならない．拡大体$\mathrm{Q}(\sqrt{a^2-4b})$，または$\mathrm{Q}(x_1-x_2)$を作ることで，二次方程式は分解される．

x_1-x_2が有理数でないとき，それが対称式ではないことが重要である．それは当然のことで，もし対称式になったら，それは基礎体に含まれることになり，ひいては係数の四則のみで解けることになるからである．

しかし，$\sqrt{a^2-4b}$を 2 乗すれはa^2-4bとなり，これは係数の四則であるから解の対称式で表せる.. 一方，x_1-x_2も，2 乗すれば,

$$(x_1-x_2)^2=x_1^2-2x_1x_2+x_2^2=x_1^2+2x_1x_2+x_2^2-4x_1x_2=(x_1+x_2)^2-4x_1x_2(=a^2-4b)$$

となって，対称式になり，基本対称式であらわすことができる！

つまり，解かれた方程式の解が基礎体にないときには，基礎体に含まれる「ある数」の平方根を追加するのであるが，そのある数とは解の対称式の平方根であり，しかもそれは解の有理式（根号を持たない）で表されるのである．上の例でいえば，ある数とは，$a^2-4b=(x_1-x_2)^2$であり，追加する平方根は$\sqrt{a^2-4b}$であり，それは同時にx_1-x_2であるということになる．

以上を一般的な定理として述べることができる．

---

[7] 例えば，二次方程式 $x^2+ax+b=0$ の基礎体を有理数体 Q とすると，$1=a/a$，$2=(a+a)/a$, 等々．

［定理４］ 方程式の解法に用いられる累乗根は，これを解の式で表すと有理式になる．

この定理は「アーベル･ルフィニの定理」を証明する上で，最も重要な前提となるものであるが，これもここでは証明しない．このように数々の重要な定理の積み重ねによって，ついに五次以上の方程式の一般的解法の不可能性が明らかになるのである．

６．これまで，二次方程式を例にあげて述べてきたが，これを一般化することで，五次以上の方程式が累乗根で解けないことの理由が明らかになる．

以下，与えられた方程式を前述の通り，

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0 \qquad \cdots ①$$

とし，その解をx_1， x_2，…， x_nとする．基礎体をＫとし，①はＫ上規約であるとする．

$n \geq 2$とし，基礎体Ｋはx_1， x_2，…， x_nをひとつも含まないので，Ｋのある要素 r を選び，そのl乗根 $\sqrt[l]{r}$ を作ってＫに追加して拡大体を作る．このrは当然$x_1, x_2, \cdots, x_n$の対称式で表すことができる．これをFとしよう．そして[定理４]によって$\sqrt[l]{r}$ は根号のない$x_1, x_2, \cdots, x_n$の有理式からできている．そこで，

$$\sqrt[l]{r} = f(x_1, x_2, ..., x_n)$$

と表すことにする． f は有理式を表わす． F と f の関係は， $F = f^l$ である．このとき，$f(x_1, x_2, ..., x_n)$は$x_1, x_2, \cdots, x_n$の対称式ではない(もし対称式なら$\sqrt[l]{r}$ はＫに含まれる)．ゆえに何か文字を入れ替えると式が変わってしまうはずである．仮にx_1とx_2を入れ替えてみよう，

$$f(x_1, x_2, ..., x_n) \neq f(x_2, x_1, ..., x_n)$$

というわけである．

しかし，$\sqrt[l]{r}$をl乗すればrにもどるから，rはFで表される．すなわち，

$$(\sqrt[l]{r})^l = r = \{f(x_1, x_2, ..., x_n)\}^l = F .$$

ところで， x_1， x_2を入れ替えたほうの$f(x_2, x_1, ..., x_n)$をl乗したらどうなるであろうか．これは同じ対称式Fになる．なぜなら，**入れ替えてからl乗するのと，l乗してから入れ替えるのとは同じこと**であり，l乗したものは対称式になるから入れ替えても同じである（例：$x_1 - x_2$と$x_2 - x_1$は異なる式だが，2 乗すれば同じ対称式になる）．見通しよくするために， $f(x_1, x_2, ..., x_n)$を単にf，$f(x_2, x_1, ..., x_n)$をf'とすると，

$$f \neq f'$$

だが，両辺をl乗すれば，

$$f^l = (f')^l = F .$$

fとf'は違う式だが，l乗すれば同じ式になるというわけである．

さて，ここで累乗根を用いる．前述した二項方程式を解く場合のように，１の原始l乗根をλ（ギリシア文字のラムダ）とすれば，

$$f = \lambda f'$$

となる．

このλは実際には 1 の何乗根なのか．それがわかれば方程式を解くときに最初に用いる累乗根がわかる．それを調べるためにこの式にもう一度x_1，x_2の入れ替えを行なってみよう．そうすると，fはf'になるが，f'はすでに入れ替わったx_1，x_2をもう一度入れ替えるのでfに戻る．ゆえに，

$$f' = \lambda f$$

となる．これを前の式に代入すると，

$$f = \lambda f' = \lambda \cdot \lambda f = \lambda^2 f$$

となるので，$\lambda^2 = 1$でなくてはならない．つまりλは1の平方根のうち，1でないほう，つまり$\lambda = -1$である．一方，λは 1 のl乗根なので$\lambda^l = 1$でなければならない．つまり，lは2の倍数であるが，lが原始的であるためには，$l = 2$でなければならない．[8]

こうして， 最初に用いる累乗根は，平方根であることがわかった．すなわち，

$$f' = -f$$

である．

以上をまとめると次のようになる．

「$n \geq 2$のとき，与えられた方程式が解けたとするなら，その分解体は，ある平方根$\sqrt{r}$を含む．それは解$x_1, x_2, \cdots, x_n$からなる有理式としてはfであり，そのfは解x_1，x_2の入れ替えを行なうと$f' = -f$に変わる．」

今，たまたまx_1とx_2の解の入れ替えによってfが$-f$に変わったが，この二つの解は$x_1, x_2, \cdots, x_n$の中のなんでもよいわけである．

このように任意の二つの文字の入れ替えによって符号が変わる式を，**交代式**という．

この，やや対称式に似た式を，交代式と呼ぶのは，一組の二文字の入れ替えで，符号が＋から－へ，あるいは－から＋に変わる(交代する)からであろうか．交代式は，文字の入れ替えで符号が変わるだけなので，2 乗すると対称式になるのが大きな特徴である．（例：$x_1 - x_2$）

さて，こうしてKに新たに追加された数$\sqrt{r}$は，平方根であることがわかったので，単に$\sqrt{r}$と表そう．新たに生成される拡大体$K(\sqrt{r})$の要素は，$a + b\sqrt{r}$(a, bはKの要素)と表されるが，これを$x_1, x_2, \cdots, x_n$の式で成り立つものとして見るならば，それは対称式と交代式から成り立つものとなっている．$a + b\sqrt{r}$のうち，a, bは対称式で，$\sqrt{r}$は交代式で表されるからである．対称式はどんな文字の入れ替えに対しても変わらないが，交代式は特定の二文字の入れ替えには符号を変えてしまう．しかし，対称式も交代式も，偶数回の二文字入れ替えにはその姿を変えないという点では同じである．

7．ここで，「文字の入れ替え」についての数学用語を導入する．

一般に，n個のものがある順序で並んでいるとき，この順序を別のものに変えることを「置換」という．例えば，1,2,3,4,5 という 5 つの数が「12345」と並んでいるものを，「24135」にするとき，これは1を2に，2を4に，3を1に，4を3に，5はそのままに置き換えているのである．特に「12345」を「21345」にするように，二つのものだけ入れ替えることを「互換」という．

置換を表す記号は，

$$\begin{pmatrix} 12345 \\ 24135 \end{pmatrix}$$

のように，カッコの中の上の行で置換の対象となる数を表し，下の行で上の数をどの数に置き換えた

---

[8] もし，$l = 4$なら，1の原始4乗根は$\pm i$であるため，$\lambda^2 = 1$にはならない．

かという結果を示す．つまりカッコ内での並び順は問わないので，

$$\begin{pmatrix}12345\\24135\end{pmatrix}=\begin{pmatrix}54321\\53142\end{pmatrix}$$

である．1 と 2 の互換のときは，

$$\begin{pmatrix}12345\\21345\end{pmatrix}$$

と書いてもよいが，特に 1 と 2 だけが入れ替えの対象なので単に（12）と表すことがある．(24)なら 2 と 4 だけの入れ替えを表わす．(12)と（21）は同じ互換を表す．

置換の記号を用いて x_1-x_2 を x_2-x_1 にすることを，

$$x_1-x_2\ |\ (12)\ =x_2-x_1$$

と表わすことにする．文字の置換を添え字の数字の置換で表現するのである．

対称式は，文字をどのように入れ替えても変わらない式であったが，それは「置換によって変わらない式」ということができる．さらに，交代式は，「ひとつの互換によって符号を変える式」ということができるが，偶数回の互換を「偶置換」ということにすれば，交代式は（対称式も）「偶置換によっては変わらない式」 ということができる．

方程式①の基礎体 K とその拡大体 K($\sqrt{r}$)の要素について，それらを解 $x_1,x_2,\cdots,x_n$ の式として表すとき，「K の要素は $x_1,x_2,\cdots,x_n$ のどんな置換によっても変わらないが，K($\sqrt{r}$)の要素は偶置換によっては変わらない」ということができる．

K($\sqrt{r}$)は，二つの解 x_1， x_2 の互換から生成されたので，方程式の解が二つだけの場合にはこれで十分である．すなわち，K($\sqrt{r}$)は二次方程式の分解体である．

しかし，K($\sqrt{r}$)は三次以上の(K 上規約な)方程式の分解体にはなりえない．このことは自明ではあるが，念のため証明してみよう．

与えられた方程式を K 上規約な三次方程式；

$$x^3+a_1x^2+a_2x+a_3=0 \qquad \cdots\cdots①'$$

とし，それが K($\sqrt{r}$)内に解を持つとすると， $x=p+q\sqrt{r}$ (p,q,r は K の要素)と表せるから， p を移行して二乗すると，

$$x-p=q\sqrt{r}$$
$$(x-p)^2=(q\sqrt{r})^2$$
$$x^2-2px+p^2-q^2r=0 \qquad \cdots\cdots②$$

となる．従って，①′ は②で割り切れるが，そのときの商は，1 次式で，それを $x-d$ とすれば，

$$x^3+a_1x^2+a_2x+a_3=(x^2-2px+p^2-q^2r)(x-d)$$

となり，両辺の係数を比較して，$a_3=q^2r\cdot d$ であるから $x-d$ は K の要素からなる式である．すなわち①′ が K 上規約であることに反する．四次以上になっても同様である．

こうして， $n\geq 3$ のときには，K($\sqrt{r}$)をさらに拡大しなければならない．解は 3 つ以上あるので，その置換には互換ではないものが存在する．互換でない置換に対して K($\sqrt{r}$)がどのように振舞うのかを調べなくてはならない．

ここで，互換でない置換として，偶置換(12)(13)を取り上げる．これは，1 と 2 を置換した後に，今度は 1 と 3 を置換することを示す．

このように互換を続けて行なうことを,数の乗法にならって「置換の乗法」といい,その結果を「積」ということにする．一般に二つの置換を続けて行なうとき，その結果をひとつの置換で表すことができる．例えば，(12)(13)では，１について見ると，最初の互換で２に変わり，その２は次の互換では変わらないので，結局１は２に変わったのである．２については，最初の互換で１に変わり，次の互換ではその１が３に変わったので結局２は３に変わった．３については，最初の互換では動かず，次の互換で１に変わっている．以上を(n個の数の)置換の「式」で表すと，

$$(12)(13)=\begin{pmatrix}123\cdots n\\213\cdots n\end{pmatrix}\begin{pmatrix}123\cdots n\\321\cdots n\end{pmatrix}=\begin{pmatrix}123\cdots n\\231\cdots n\end{pmatrix}.$$

となる．最後の結果を表しているのが置換の「積」というわけである．

さらに，この積を見ると，1→2→3→1 というように数が循環しているので，これを (123) と表せば，互換(12)と同様な簡略表現ができる．すなわち，

(12)(13)＝(123)

というわけである．この右辺のような置換を「循環置換」と呼ぶ．互換は一番短い循環置換である．ただし，(13)(24)のように二つの互換に共通の数字がないときには，これをひとつの循環置換で表すことはできない．逆に，互換よりも長いどのような循環置換も，それをより短い循環置換の積で表すことができる(ただし，その表し方は一意的ではない).

結局，あらゆる置換を，互換だけの乗法の式で表すことができ，そのときの互換の個数が偶数個ならば，それは偶置換であり，奇数個ならば「奇置換」という．ちなみにこの偶奇性はその表し方に拠らない．すべての置換は，偶置換または奇置換である．

例：(1234)＝(12)(13)(14)＝(12)(34)(13)　(奇置換).

(13245)＝(132)(145)＝(13)(12)(14)(15) =(13)(12)(45)(14)　(偶置換),

８．さて，話を方程式に戻す.

$n\geq 3$のとき，少なくともx_1,x_2,x_3の解が存在するので，偶置換 (123) が可能となる． K($\sqrt{r}$)の要素は，$x_1,x_2,\cdots,x_n$の式としてみれば偶置換によっては変わらないはずなので，そのなかのある要素sを取り，そのm乗根$\sqrt[m]{s}$を K($\sqrt{r}$)に追加し，新たな拡大体 K($\sqrt{r}$，$\sqrt[m]{s}$)を構成する．ここから先は$\sqrt{r}$を導入するときと同様の方法でmを求める.

[定理 4]によって，$\sqrt[m]{s}$を解$x_1,x_2,\cdots,x_n$で表すと，ある有理式$g(x_1,x_2,x_3,\cdots,x_n)=g$になる．すなわち,

$$\sqrt[m]{s}=g(x_1,x_2,x_3,\cdots,x_n)=g\,.$$

これは K($\sqrt{r}$)の要素ではないから偶置換によって変化する．すなわち，偶置換(123)を適用すると別の式になるから，これをg’で表せば,

$$g(x_1,x_2,x_3,\cdots,x_n)\ |\ (123)=g(x_2,x_3,x_1,\cdots,x_n)=g'$$

となる．当然,

$$g\neq g'$$

であるが，gをm乗すれば K($\sqrt{r}$)の要素(＝s)になり，偶置換で変わらない式となるから,

$g^m \mid (123) = g^m$

である．一方，g’については，**gを(123)で偶置換したあとにm乗するのと，m乗してから偶置換するのは同じ**ことなので，g’をm乗すれば，g^mと同じものになる．つまり，

$$\left(g' \right)^m = g^m$$

となる．従って，また1の原始m乗根が登場して(これをμ(ギリシア文字のミュー)で表す)，

$$g' = \mu g \qquad (\mu^m = 1,\ \mu \neq 1)$$

となる．すなわち，

$$g(x_2, x_3, x_1, \cdots, x_n) = \mu\ g(x_1, x_2, x_3, \cdots, x_n) \qquad \text{(A)}$$

この両辺に偶置換(123)を適用すると，

$$g(x_2, x_3, x_1, \cdots, x_n) \mid (123) = \mu\ g(x_1, x_2, x_3, \cdots, x_n) \mid (123)$$

$$g(x_3, x_1, x_2, \cdots, x_n) = \mu\ g(x_2, x_3, x_1, \cdots, x_n) \qquad \text{(B)}$$

(B)の右辺の$g(x_2, x_3, x_1, \cdots, x_n)$は(A)の左辺と同じだから，(A)の右辺を(B)の右辺に代入すると，

$$\begin{aligned} g(x_3, x_1, x_2, \cdots, x_n) &= \mu\ g(x_2, x_3, x_1, \cdots, x_n) \\ &= \mu \cdot \mu\ g(x_1, x_2, x_3, \cdots, x_n) \\ &= \mu^2\ g(x_1, x_2, x_3, \cdots, x_n) \end{aligned} \qquad \text{(C)}$$

ここでもう一度，偶置換(123)を行なうと．

$$g(x_1, x_2, x_3, \cdots, x_n) = \mu\ g(x_3, x_1, x_2, \cdots, x_n) \qquad \text{(D)}$$

(D)の左辺はすなわちgであり，右辺の$g(x_3, x_1, x_2, \cdots, x_n)$は(C)の式の左辺と同じであるから，これの替りに(C)の右辺$\mu^2\ g(x_1, x_2, x_3, \cdots, x_n)$を代入できる．従って，

$$g(x_1, x_2, x_3, \cdots, x_n) = \mu^3\ g(x_1, x_2, x_3, \cdots, x_n)$$

すなわち，

$$g = \mu^3\ g$$

こうして，$\mu^3 = 1$が導かれる．一方，$\mu^m = 1$よりmは3の倍数であり，また原始的であることから$m = 3$となる．μは1の原始三乗根ωそのものである．

こうして，K($\sqrt{r}$)に新たに追加される数$\sqrt[m]{s}$は三乗根$\sqrt[3]{s}$であることがわかった．

ここでひとつ，注意すべきこととして，1の原始累乗根の体への追加の問題がある．K($\sqrt{r}$)の場合には，1の平方根(＝－1)だったので，これはもともとKに存在し，ことさら追加する必要はなかったが，今度は1の原始三乗根ωなので，これは$\sqrt[3]{s}$とは別に，独自にK($\sqrt{r}$)に追加されねばならない．従って，新たに生成される体は，K($\sqrt{r}$，$\sqrt[3]{s}$，ω）ということになる．

9．ここでひとつ，実際の三次方程式の解法に基づいて上の理論を振り返ってみよう．

与えられた方程式を，前述どおり，

$$x^3 + a_1 x^2 + a_2 x + a_3 = 0 \qquad \cdots\cdots ①'$$

とする．三次方程式の一般的な解法は高校数学の範囲外なので，以下簡単に説明する．

仮に，$x=y+A$ とおいて①′に代入すると，x^3 の項の展開からは，「$3Ay^2$」が表われ，a_1x^2 の項の展開からは，「a_1y^2」が表われるので，$-3A=a_1$ となるように A を決めてやれば，y の二次の項が消えるはずである．すなわち，$x=y-\dfrac{a_1}{3}$ として，代入・展開することで，

$$y^3+ay+b=0 \qquad \cdots\cdots①''$$

とすることができる．ちなみに，

$$a=-\frac{a_1^2}{3}+a_2,\quad b=\frac{2a_1^3}{27}-\frac{a_1a_2}{3}+a_3$$

である．さて，①”が解ければ，①′も解けるが，ここで前述した「解と係数の関係」から，①”の三つの解を仮に，y_1，y_2，y_3 とすると，二次の項の係数が０であることから，

$$y_1+y_2+y_3=0 \qquad \cdots\cdots①''$$

となる．これから，$y_1=-y_2-y_3$ となって，ひとつの解を他の二つの解の和で表せることに着目する．そこで改めて，u，v を任意の数として，$y=u+v$ とおいて，①”に代入・展開・整理すれば，

$$(u^3+v^3+b)+(u+v)(3uv+a)=0$$

となる．この式で，$u^3+v^3+b=0$，$3uv+a=0$ が成り立つように u，v を決めてやれば上の式も成り立つ．すなわち，

$$\begin{cases} u^3+v^3=-b \\ u^3v^3=-\dfrac{a^3}{27} \end{cases}$$

を満たすような u，v であるが，これは u^3，v^3 についての二次方程式になっている！

この方程式は，和が $-b$，積が $-a^3/27$ であるような二つの数を求めることだから，方程式；

$$t^2+bt-\frac{a^3}{27}=0$$

の解である．これにより，$t=\dfrac{-b\pm\sqrt{b^2-\dfrac{4a^3}{27}}}{2}=-\dfrac{b}{2}\pm\sqrt{\dfrac{b^2}{4}+\dfrac{a^3}{27}}$ が得られ，ここから

$$u^3=-\frac{b}{2}+\sqrt{\frac{b^2}{4}+\frac{a^3}{27}},\quad v^3=-\frac{b}{2}-\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}$$

が得られる．あとはこの三乗根を取って，

$$u=\sqrt[3]{-\frac{b}{2}+\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}},\quad v=\sqrt[3]{-\frac{b}{2}-\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}}\ .$$

もちろん，三乗根 u，v はそれぞれ３つずつある(u，ωu，ω^2u 等)ので，$3uv+a=0$ を満たすように決める．こうして，$y=u+v$ から y が得られ，$x=y-\dfrac{a_1}{3}$ から x が得られる．

三次方程式だけでも実は多くのことを述べなければならないが，取りあえずは，こうして解(のひとつ)を求めることができる．

以上の解法で，まずa，bは，基礎体Kの要素であるa_1，a_2，a_3から四則で作り出された数であるから K の要素であり，従って，$\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}$が，K に最初に追加される平方根$\sqrt{r}$にあたり，$u=\sqrt[3]{-\frac{b}{2}+\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}}$が次に追加される三乗根$\sqrt[3]{s}$にあたる．こうして三次方程式①”の分解体；

$$\mathrm{K}\left(\sqrt{\frac{b^2}{4}+\frac{a^3}{27}},\ \sqrt[3]{-\frac{b}{2}+\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}},\ \omega\right)$$

が生成される．もともとの方程式①′の分解体も同じものである．

10. $n=4$のとき，すなわち，四次方程式の場合はどうであろうか．これも例を挙げて述べてみよう．今度は係数も具体的に決めて，

$$x^4+4x^3+7x^2+2x-5=0 \qquad \cdots\cdots①^\circ$$

とする．係数を決めたのは文字式の場合の見た目の煩雑さを避けるためである．

$x=y-1$とおくことで，三次方程式と同様に３次の項を消去することができる． これを①°に代入･展開・整理すると，

$$y^4+y^2-4y-3=0 \qquad \cdots\cdots⑧$$

となる．ここで，

$$y^4=-y^2+4y+3$$

と，２次以下を右辺に移項してから，二次方程式の解法をまねて，両辺を完全平方化するためのテクニックを用いる．新たな未知数としてzを用い，両辺に$2zy^2+z^2$を加えるのである．

$$y^4+2zy^2+Z^2=-y^2+4y+3+2zy^2+z^2$$

こうすると，左辺は，$\left(y^2+z\right)^2$と平方化できる．右辺もまとめて，

$$\left(y^2+z\right)^2=(2z-1)y^2+4y+\left(z^2+3\right) \qquad \cdots\cdots⑨$$

ここで右辺も完全平方化できるようにするには，このyの二次式の判別式Dを０とするようにzを決めればよいことになる．すなわち，

$$D/4=2^2-(2z-1)(z^2+3)=0$$

$$\therefore\ 2z^3-z^2+6z-7=0$$

この式は三次方程式であるから解ける．というよりも，因数定理を用いて$z=1$がその解のひとつであることが容易にわかるので，これを⑨に代入すれば，

$$\left(y^2+1\right)^2=y^2+4y+4$$

$$\therefore\ y^2+1=\pm(y+2)$$

$y^2+1=y+2$，$y^2+1=-y-2$から，それぞれ，

$$y=\frac{1\pm\sqrt{5}}{2},\quad \frac{-1\pm\sqrt{-11}}{2}$$

が出てくる．そして，$x=y-1$ であったから，

$$x=\frac{1\pm\sqrt{5}}{2}-1=\frac{-1\pm\sqrt{5}}{2},\quad \frac{-1\pm\sqrt{-11}}{2}-1=\frac{-3\pm\sqrt{-11}}{2}$$

という，４つの解が得られる．これが正しいことは，①゜に代入してみればわかる．

四次方程式が基礎体 K のなかに一つも解を持たない場合，上記のように完全平方化の条件から三次方程式が出てくる．これは四次方程式を解くための「分解方程式」と呼ばれるものであるが，この分解方程式の係数体は見てわかるように K の域を出ない．しかも，分解方程式が K 上可約なときには，上記の例題のように，あたかも二次方程式を解くように，比較的簡単にもとの四次方程式が解かれる．この場合は K の拡大は二次方程式の場合と同様，$\sqrt{r}$ による拡大のみでよい．しかし，一般には分解方程式は K 上既約と考えるべきなので，これを解くために三次方程式のときと同様，さらに $\sqrt[3]{s}$ による拡大も必要となるのである．

11．さて，$n=5$ のときにも，累乗根による解法が可能だとして，これまでの議論同様，K($\sqrt{r}$) に対して $\sqrt[m]{s}$ を追加し，それに偶置換(123)を適用したとして，拡大体 K($\sqrt{r}$，$\sqrt[3]{s}$，ω)を生成できたと仮定する．しかし解が５つ以上あるときの偶置換は，このような拡大を許さないのである．

仮定によって，s は偶置換 (123) によって変わらないが，$\sqrt[3]{s}=g(x_1,x_2,x_3,\cdots,x_n)$ は g ’ に変化する．ところで，置換(13245) は前述(「７．」末尾)のように偶置換であるから，(123)と同様に s は変わらないが，$\sqrt[3]{s}$ は変わらなければならない．その様子を見よう．

まず，(13245)＝(132)(145) であることを確認する．

そして，最初に偶置換(132)によって $\sqrt[3]{s}$ はどう変わるか．実は前回と同じである．前回は偶置換の例として(123)を用いたが，それは別に，(132)でも(145)でもよかったのである．だから，$g(x_1,x_2,x_3,x_4,x_5)$ に，(132)を適用しようが，(145)を適用しようが，結果は $\omega\cdot g$ になるだけである．というのは，(132)の適用によって $\omega\cdot g$ となったあと，(145)の適用によって $\omega\cdot\omega\cdot g=\omega^2\cdot g$ となるが，ω と ω^2 はともに 1 の原始立方根であり，本質的には同じものである（「３．」参照）．したがって，$g(x_1,x_2,x_3,x_4,x_5)$ に (13245) を適用しても $\omega\cdot g$ になるだけなのである．こうして，

$$g(x_1,x_2,x_3,x_4,x_5)\ |(13245)=\omega\cdot g(x_1,x_2,x_3,x_4,x_5)$$

左辺は，x_1 は x_3 に，x_3 は x_2 に，x_2 は x_4 に，x_4 は x_5 に，x_5 は x_1 に置換されるから，

$$g(x_3,x_4,x_2,x_5,x_1)=\omega\cdot g(x_1,x_2,x_3,x_4,x_5)\qquad (A)$$

この両辺に再度(13245)を適用すると，

$$g(x_2,x_5,x_4,x_1,x_3)=\omega\cdot g(x_3,x_4,x_2,x_5,x_1)\qquad (B)$$

(B)に(A)を代入すると，

$$g(x_2,x_5,x_4,x_1,x_3)=\omega^2\cdot g(x_1,x_2,x_3,x_4,x_5)\qquad (C)$$

この両辺にさらに (13245) を適用すると，

$$g(x_4,x_1,x_5,x_3,x_2)=\omega^2\cdot g(x_3,x_4,x_2,x_5,x_1)\qquad (D)$$

(D)に(A)を代入すると，

$$g(x_4,x_1,x_5,x_3,x_2)=\omega^3\cdot g(x_1,x_2,x_3,x_4,x_5) \qquad \text{(E)}$$

もう一回，(13245) を適用すると，

$$g(x_5,x_3,x_1,x_2,x_4)=\omega^3\cdot g(x_3,x_4,x_2,x_5,x_1) \qquad \text{(F)}$$

(F)に(A)を代入すると，

$$g(x_5,x_3,x_1,x_2,x_4)=\omega^4\cdot g(x_1,x_2,x_3,x_4,x_5) \qquad \text{(G)}$$

最後にもう一回，(13245) を適用すると，

$$g(x_1,x_2,x_3,x_4,x_5)=\omega^4\cdot g(x_3,x_4,x_2,x_5,x_1) \qquad \text{(H)}$$

(H)に(A)を代入して，いよいよ完成である．

$$g(x_1,x_2,x_3,x_4,x_5)=\omega^5\cdot g(x_1,x_2,x_3,x_4,x_5) \qquad \text{(H)}$$

最後の式から得られる結論は，$\omega^5=1$ でなければならないということである．ところが，すでに解明したとおり，ω は 1 の原始三乗根で，かつ$\omega\neq 1$ であるから，$\omega^5=1$にはなり得ない．

逆に，$\omega^5=1$とするならば，$\omega^3=1$でもあることから，$\omega=1$ でなければならない．すると，$g(x_1,x_2,x_3,x_4,x_5)$ は，偶置換(13245)では変わらないことになる．$g^3(=s)$ は偶置換で変わらない式であったが，$g\,(=\sqrt[3]{s})$も変わらない式ということになるのである．

さらに，(13245) で変わらないならば，同様に偶置換 (32154) でも変わらないであろう．何故この式を出したかというと，

(13245)(32154)＝(123)

だからで，この左辺のふたつの置換によってg が変わらないならば，右辺の(123)によっても変わらないことになり，これは，これまでの議論の根拠としてきた，「K($\sqrt{r}$, $\sqrt[3]{s}$, ω)の要素は，$x_1,x_2,\cdots,x_n$ の式としては偶置換によって変わる」ということと矛盾するのである．

これが，五次方程式，ひいては五次以上の方程式が累乗根では一般的に解けないことの理由となる．すなわち，五つ以上の解$x_1,x_2,\cdots,x_n$ で$g\,(=\sqrt[3]{s})$を表したとき，それが偶置換によって変わりながら，同時に$g^3(=s)$では変わらないようにはできないということである．

---

12. あとがき

これまでの議論は，「アーベル・ルフィニの定理」の直接の証明として用いられる論法であるが，現在では，この定理は，もっと広い「ガロアの理論」の応用として述べられるのが普通である．それは，上述の置換を「群」というさらに広い数学概念によって捕らえ(「置換群))，その性質を極めることで得られるものである．すなわち，一つひとつの方程式に固有の「群」が存在し，その「群」が「可解性」という性質を持つとき，その方程式は累乗根による解法が可能である，というものである．

しかし，五次以上の代数方程式に属する「群」が，一般的にはその「可解性」という性質を持たないことの証明には，上述の(「11.」の)議論を敷衍(ふえん)することが必要である．従ってこの議論がすでに過去のものとなってしまったというのは，浅薄な早計と言わざるを得ない．

2009 年 8 月 25 日

福沢正男

13. 参考にした本など

高木貞治「代数学講義」改訂新版 25 刷 共立出版株式会社(1994 年)
高木貞治「復刻版　近世数学史談・数学雑談」復刻版 1 刷　共立出版株式会社(1996 年)
「基礎数学口座」1 巻　奥川光太郎「代数学」初版 22 冊　共立出版株式会社(昭和 46 年)
矢ケ部巌「数Ⅲ方式　ガロアの理論」2 版　株式会社 兼文堂(1978 年)