富山大学教育学部紀要Ｂ（理科系）№40：１－10（平成四年）

代数方程式論（Ⅰ）

浅沼　照雄

（1991年10月21日受理）

A Theory of Algebraic Equations（Ⅰ）

Teruo ASANUMA

はじめに

大学における学部，学科で数学の一分科である代数学をそのカリキュラムとして系統的に組んでいるのは理学部数学科，教育学部（数学専攻）及びこれに類する学部，学科等である。そのカリキュラムの中で代数方程式論はガロア理論の中で取り扱われる。たとえば近代代数学の主要な結果の一つである５次方程式の代数的解法は不可能であることの証明はガロア理論を用いて示される。しかしガロア理論は群，環，体など代数系の理論の一つの柱であって，きわめて抽象的かつ大掛りの準備を必要とする。特にその抽象性のゆえ高校数学とのギャップは大きく，その修得については多大の努力を要求するものである。

このギャップをすこしでも埋めるという目的のため，代数方程式論を歴史的な順序から見て，現代の抽象的なガロア理論の登場以前の16世紀から19世紀の前半に至るフォンタナ（通称タルタリア），カルダノ，ラグランジュ，ルフィニ，アーベル等の理論を初等的に考察するということは一つの方法と思われる。このような立場から代数方程式論を展開していく。目標はルフィニ，アーベル等による「５次以上の代数方程式の代数的解法が不可能であること」[（１）を参照]である。

本論文ではこの証明に必要な基礎理論を出来るかぎり初等的に与えるのが目的である。

１．２次方程式

中学校教育において２次方程式とはａ，ｂ，ｃを実数として

$$ax^2+bx+c=0 \quad (a\neq 0)$$

なる形をした方程式である。この両辺をａで割って

$$x^2+a^{-1}bx+a^{-1}c=0$$

を得る。ゆえ$a^{-1}b$，$a^{-1}c$をあらためてａ，ｂとおけば２次方程式を解くためには

$$x^2+ax+b=0 \qquad (1)$$

なる形の方程式を考えれば十分である。よく知られているようにこの方程式の根の公式は$D=a^2-4b$とおいて

$$x=(-a\pm\sqrt{D})/2 \qquad (2)$$

で与えられる。この意味はａ，ｂにいかなる実数代入しても（２）は（１）をみたすということである。$a^2-4b=D$が実数の場合，２乗根$\sqrt{D}$の意味は明解であり，これが高等学校で複素数が導入された後も，２次方程式は実数係数の場合のみを取扱っている理由の一つであろう。

（１）においてａ，ｂが複素数であるときＤは一般には実数でない。このとき$\sqrt{D}$がいかなる意味をもつかは重要である。この場合$\sqrt{D}$は一つには

定まらない。すなわち$\sqrt{D}$は2項方程式$x^2-D=0$の2つの根のうち一つを表わしているのである。それゆえ$\sqrt{\ }$の意味は中にはいるDが実数であるときとそうでないときは違っていることに注意する。

さて（2）を根と係数の関係を用いて与えてみよう。

$$f(x)=x^2+ax+b$$

とおいて$f(x)=0$の2根をx_1，x_2とする。根と係数の関係から

$$-a=x_1+x_2,\quad b=x_1x_2$$

がなりたつ。

$$x_1=\{(x_1+x_2)+(x_1-x_2)\}/2$$
$$x_2=\{(x_1+x_2)-(x_1-x_2)\}/2$$

であって

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

に注意すれば、x_1-x_2は2項方程式

$$X^2=(x_1-x_2)^2=a^2-4b=D$$

の一つの根である。ゆえ$x_1-x_2=\sqrt{D}$と表わせて

$$\begin{cases}x_1=(-a+\sqrt{D})/2\\ x_2=(-a-\sqrt{D})/2\end{cases}\qquad(3)$$

を得る。

上の議論においてx_1，x_2を不定元（又は文字）と考えれば2次方程の根の公式とはx_1，x_2を基本対称式x_1+x_2，x_1x_2およびベキ根（又は根号）$\sqrt{\ }$を用いて表わす式のことである。

根の公式（3）には2乗根$\sqrt{D}$が用いられている。このベキ根を用いない根の公式，すなわちa，b，の有理式のみで根の公式がつくれるかどうかを考えてみよう。

（注．a，bの有理式とはaとbを不定元とした2つの整式　$F(a,b)$，$G(a,b)$の商$F(a,b)/G(a,b)$（$G(a,b)\neq 0$）のことである。）

不定元x_1，x_2が$f(x)=0$の2根とし，

$$x_1=\Phi(a,b)=a,\ b\text{の有理式}$$

とする。この式のx_1，x_2を交換するとx_1はx_2に変わる。一方a，bは変らないから当然$\Phi(a,b)$もかわらない。ゆえ

$$x_2=\Phi(a,b)=x_1$$

となり矛盾。すなわち2次方程式の根の公式には根号が必要である。

2．3次方程式

3次方程式とは

$$ax^3+bx^2+cx+d=0\quad(a\neq 0)$$

なる形をした方程式で，係数a，b，c，dは一般には複素数である。2次方程式の場合と同様，この方程式の解を得るためには両辺をaで割って，x^3の係数は1としてよい。すなわち初めから

$$x^3+ax^2+bx+c=0$$

としてよい。カルダノの解法を用いてこの方程式の根の公式を求めてみよう。まず求める方程式の根をx_1，x_2，x_3とする。すると根と係数の関係から

$$\begin{cases}-a=x_1+x_2+x_3\\ b=x_1x_2+x_2x_3+x_3x_1\\ -c=x_1x_2x_3\end{cases}$$

を得る。問題はx_1，x_2，x_3をa，b，c及びベキ根を用いて表わすことである。ただしこの場合は根号として，2乗根だけでなく3乗根も用いる。

まず，

$f(x)=x^3+ax^2+bx+c$，$x=y-\frac{1}{3}a$

とおくと

$$f(y-\tfrac{1}{3}a)=y^3+\alpha y+\beta$$
$$(\alpha=-\tfrac{1}{3}a^2+b,\ \beta=\tfrac{2}{27}a^3-\tfrac{1}{3}ab+c)$$

となる。そこで

$$\begin{cases}A=27(-\frac{1}{2}\beta+\frac{1}{2}(\beta^2+\frac{4}{27}\alpha^3)^{1/2})\\ B=27(-\frac{1}{2}\beta-\frac{1}{2}(\beta^2+\frac{4}{27}\alpha^3)^{1/2})\end{cases}$$

とおく。さて$A^{1/3}(=\sqrt[3]{A})$で$X^3=A$の1根，すなわち，Aの3乗根を表わす。ゆえAの3乗根は3つあって他の2つはωを$\omega^2+\omega+1$の根とするとき，$\omega A^{1/3}$，$\omega^2A^{1/3}$と表わされる。

$A^{1/3}B^{1/3}$は$AB=-27\alpha^3$の3乗根の一つであるから-3α，$-3\alpha\omega$，$-3\alpha\omega^2$のどれかである。もし$A^{1/3}B^{1/3}=-3\alpha\omega$ならばA，Bそれぞれの3乗根$A^{1/3}$，$B^{1/3}$のかわりに$\omega A^{1/3}$，$\omega B^{1/3}$をとれば

$$(\omega A^{1/3})(\omega B^{1/3})=-3\alpha\omega^3=-3\alpha$$

がなりたつ。同様に$A^{1/3}B^{1/3}=-3\alpha\omega^2$のときは$A^{1/3}$，$B^{1/3}$のかわりに$\omega^2A^{1/3}$，$\omega^2B^{1/3}$を選べば

$$(\omega^2A^{1/3})(\omega^2B^{1/3})=-3\alpha\omega^6=-3\alpha$$

とできる。ゆえ最初から$A^{1/3}$，$B^{1/3}$を$A^{1/3}B^{1/3}=$

-3αなるよう選んでおけば
$\frac{1}{3}(A^{1/3}+B^{1/3}),\frac{1}{3}(\omega^2A^{1/3}+\omega B^{1/3}),\frac{1}{3}(\omega A^{1/3}+\omega^2B^{1/3})$
がyについての3次方程式

$$y^3+\alpha y+\beta=0$$

の3根となる。たとえば簡単な計算より

$$\{\tfrac{1}{3}(A^{1/3}+B^{1/3})\}^3+\alpha(A^{1/3}+B^{1/3})\}+\beta=\tfrac{1}{27}(A+B)+\beta+(\tfrac{1}{9}A^{1/3}B^{1/3}+\tfrac{1}{3}\alpha)(A^{1/3}+B^{1/3})\quad(4)$$

ここで，$A+B=-27\beta$，$A^{1/3}B^{1/3}=-3\alpha$
を代入すれば（4）は0となる。

（注．$A^{1/3}$，$B^{1/3}$を$A^{1/3}B^{1/3}=-3\alpha$なるように選ぶ理由はここにある。）

他の2根についても同様にして確かめることができる。求める方程式の3根は

$$x=y-(1/3)a$$

より

$$\begin{cases}x_1=\frac{1}{3}(A^{1/3}+B^{1/3}-a)\\ x_2=\frac{1}{3}(\omega^2A^{1/3}+\omega B^{1/3}-a)\\ x_3=\frac{1}{3}(\omega A^{1/3}+\omega^2B^{1/3}-a)\end{cases}\quad(5)$$

と表わせる。

ここで使われているベキ根は

$$(\beta^2+\tfrac{4}{27}\alpha^3)^{1/2},\ A^{1/3},\ B^{1/3}$$

である。

さてこの3つのベキ根について次に述べるように，注目すべき事実がなりたつ。

まず，$\omega^2+\omega+1=0$であるから

$$\begin{cases}A^{1/3}=x_1+\omega x_2+\omega^2x_3\\ B^{1/3}=x_1+\omega^2x_2+\omega x_3\end{cases}$$

がなりたつ。つまり$A^{1/3}$，$B^{1/3}$はx_1，x_2，x_3の有理式として表わされてる。

次に

$\Delta=(x_1-x_2)(x_1-x_3)(x_2-x_3)$＝差積とおけば，$\Delta^2=-4\alpha^3-27\beta^2$がなりたつ［たとえば（2，P．59)]。ゆえに$(\sqrt{-3}/9)\Delta$は$\beta^2+(4/27)\alpha^3$の2乗根となる。ゆえカルダノの公式（5）に表われるベキ根はすべて根x_1，x_2，x_3の有理式となっていることに注意する。

ルフィニはこの点に注目し5次以上の代数方程式の代数的解法が不可能なることの証明の道筋を見つけたのであった。

4次方程式に対する解の公式又は解法はフェラリによって与えられているがここで省略する［フェラリの公式については（2，P．70）参照］。

以下ルフィニ，アーベルによる5次以上の代数方程式について，代数的解法が存在しないことの証明の準備をする。

3．有理式と四則

X_1,X_2,X_3,X_4,X_5を不定元（又は文字）とする。$\phi(X_1,X_2,X_3,X_4,X_5)=\phi(X_1,\cdots,X_5)=\phi$が有理式であるとは$\phi$が2つの整式f，gの商，f／g（$g\neq0$）で表わされていることである。この場合，一般的には係数は複素数（もちろん実数も含んでいる）まで考えておく。

さてϕとψを2つの有理数とする。すると

$\phi\pm\psi$　（和及び差），$\phi\psi$（積）

はまた有理式である。更に，$\psi\neq0$ならば

$$\phi\psi^{-1}=\phi/\psi$$

も有理式であることが簡単に確あめられる。すなわち有理式の全体は，有理数の全体と同様に四則（四則演算，すなわち加減乗除又は和差積商）が可能である。

Cで複素数の集合を表わしたとき

$C(X_1,X_2,X_3,X_4,X_5)$又は$C(X_1,\cdots,X_5)$

などで有理式ϕの全体の集合を表わす。

$$K=C(X_1,\cdots,X_5)$$

とおいて上記のことをKを用いて表わせば

$K\ni\phi,\psi\Rightarrow K\ni\phi\pm\psi,\phi\psi$更に$\psi\neq0$ならば

$$K\ni\phi\psi^{-1}$$

となる。このKのように四則が可能な集合を有理区域又は体という。

さて$K=C(X_1,\cdots,X_5)$の元ϕについて，ϕのp乗根，$\phi^{1/p}(=\sqrt[p]{\phi})$を考える。ここでpは素数とする。$\varepsilon$を1のp乗根（すなわち$\varepsilon^p=1$）で$\varepsilon\neq1$なるものとする。すると不定元Xについて

$$X^p-\phi=(X-\phi^{1/p})(X-\varepsilon\phi^{1/p})\cdots(X-\varepsilon^{p-1}\phi^{1/p})\quad(6)$$

と因数分解されるから，ϕのp乗根は

$$\phi^{1/p},\ \varepsilon\phi^{1/p},\ \varepsilon^2\phi^{1/p},\cdots,\varepsilon^{p-1}\phi^{1/p}$$

のp個である。

（注．上の$\phi^{1/p}$の記述は現代数学の立場からみると厳密ではない。正確に述べるとKの代数的閉体を一つ固定しておいて，その中で$\phi^{1/p}$を考え

るのであるが，その証明は初等的でない。実際，アーベルの論文においてもその点があいまいである。

しかし$\phi^{1/p}$の存在定理をはぶいたとしても理論の大筋は失われないと思われる。)

$$\Phi = a_0 + a_1\phi^{1/p} + \cdots a_{p-1}\phi^{(p-1)/p} \qquad (7)$$
$$(a_i \in K,\ i = 0, \cdots,\ p-1)$$

の形の元のなす集合を

$$C(X_1, \cdots, X_s,\ \phi^{1/p}) \text{ 又は } K(\phi^{1/p})$$

で表わす。すると次のことは容易に示される。

$K(\phi^{1/p}) \ni \Phi, \Psi \Rightarrow K(\phi^{1/p}) \ni \Phi \pm \Psi,\ \Phi\Psi$。

すなわち$K(\phi^{1/p})$の中で和，差，積が可能である。次に$\Psi \neq 0$として商$\Phi\Psi^{-1}$が$K(\phi^{1/p})$に含まれることを示そう。このためには$\phi^{1/p} \notin K$のとき$\Psi^{-1} \in K(\phi^{1/p})$を示せば十分である。なぜならば上に述べたことより

$K(\phi^{1/p}) \ni \Phi,\ \Psi^{-1} \Rightarrow K(\phi^{1/p}) \ni \Phi\Psi^{-1}$

がなりたつからである。まずΦを（7）のようにおいて整式

$$F(Y_i) = a_0 + a_1 Y_i^{1/p} + \cdots a_{p-1} Y_i^{(p-1)/p}$$
$$(i = 0, \cdots, p-1)$$

を考える。ここで

$$G = F(Y_0)F(Y_1)\cdots F(Y_{p-1})$$

とおくと簡単な計算によってGはKの元を係数とする$Y_0, \cdots, Y_{p-1}$の整式である。

(注. この計算ができることはKの任意の元に対して四則が定義されている，すなわちKは体であるからである。)

Gの不定元$Y_0, \cdots, Y_{p-1}$の中のどの2つを交換してもGは変化しないからGは対称式である。ゆえ

$$S_1 = Y_1 + \cdots + Y_{p-1}$$
$$S_2 = Y_0Y_1 + \cdots + Y_{p-2}Y_{p-1}$$
$$\vdots$$
$$S_p = Y_0Y_1\cdots Y_{p-1}$$

を$Y_0, \cdots, Y_{p-1}$の基本対称式とすると，GはKの元を係数とする$S_1, \cdots, S_p$の整式である〔対称式についてはたとえば（2，p．52）を参照〕。

他方ε（$\neq 1$）を1のp乗根の一つとすると（6）の根と係数の関係より，$S_1, \cdots, S_p$の各Y_iに$\varepsilon^i\phi^{1/p}$を代入した値，$S'_1, \cdots, S'_p$について

$$S'_1 = S'_2 = \cdots S'_{p-1} = 0,\ S'_p = \phi$$

がなりたつ。ゆえにGの各Y_iに$\varepsilon^i\phi^{1/p}$を代入したものをG'とかくと明らかにKの元である。すなわち

$$G' = F(\phi^{1/p})F(\varepsilon\phi^{1/p}) \cdots F(\varepsilon^{p-1}\phi^{1/p}) \in K$$

がなりたつ。ゆえに$G'^{-1} \in K$である[1]。

一方簡単のため，$F_i = F(\varepsilon^i\phi^{1/p})(i = 0, \cdots, p-1)$

とおけば

$$\Phi^{-1} = F_0^{-1} = F_1F_2\cdots F_{p-1} / F_0F_1\cdots F_{p-1}$$
$$= G'^{-1}F_1F_2\cdots F_{p-1}$$

である。ここで$G'^{-1} \in K$であるから当然G'^{-1}は$K(\phi^{1/p})$の元でもある。ゆえΦ^{-1}は$K(\phi^{1/p})$の元G'^{-1}，$F_1, \cdots, F_{p-1}$の積となり前に述べたことからΦ^{-1}自身も$K(\phi^{1/p})$の元となる。

以上をまとめると$K(\phi^{1/p})$内で四則が可能である，すなわち$K(\phi^{1/p})$は体である。

次に$\phi^{1/p} \notin K$ならばΦの（7）による表現が一意，的であることを示そう。すなわち

$$\Phi = a_0 + a_1\phi^{1/p} + \cdots + a_{p-1}\phi^{(p-1)/p}$$
$$= b_0 + b_1\phi^{1/p} + \cdots + b_{p-1}\phi^{(p-1)/p}$$
$$(a_i, b_i \in K,\ i = 0, \cdots,\ p-1)$$
$$\Rightarrow\ a_i = b_i\ (i = 0, \cdots,\ p-1) \qquad (8)$$

を示せばよい。

そのためにまずユークリッドの互除法について述べる。ユークリッドの互除法とはもともと整数の最大公約数を求める方法として知られてきた。又同様のことが数を係数とする一変数の整式についてもなりたつ。すなわち$f(X)$，$g(X)$を2つの整式として$g(X) \neq 0$と仮定する。そこで$f(X)$を$g(X)$で割って

$$f(X) = q_1(X)g(X) + r_1(X)$$
$$(\deg r_1(X) < \deg g(X))$$

とおける。ここで$\deg g(X)$はXの次数を表わす同様にして$g(X)$を$r_1(X)$で割って

$$g(X) = q_2(X)r_1(X) + r_2(X)$$
$$((\deg r_2(X) < \deg r_1(X))$$

この繰作を続けて

$$r_1(X) = q_3(X)r_2(X) + r_3(X)$$
$$(\deg r_3(X) < \deg r_2(X))$$
$$\vdots$$

$r_{n-1}(X)=q_{n+1}(X)r_n(X)+r_{n+1}(X)$
$(\deg r_{n+3}(X)<\deg r_{n+2}(X))$
$r_n(X)=q_{n+2}(X)r_{n+1}(X)$
を得る。この最後の整式 $r_{n+1}(X)$ が $f(X)$ と $g(X)$ の最大公約数（又は最大公約式）となる。またこの式の列より
$h(X)f(X)+k(X)g(X)=r_{n+1}(X)$
なる整式を求めることができる［くわしくは（2，p. 20）参照］。

上のような，整式に対するユークリッドの互除法について，もっとも重要なことは整式の係数について四則を用いているだけである事実に注意することである。すなわち整式 $f(X)$ 及び $g(X)$ の係数が K や $K(\phi^{1/p})$ など四則が可能なる集合(体) の元であればユークリッドの互除法がおこなえるという点に注意する。

さて（8）を示すためにまず次の補題を証明する。

補題. $\phi^{1/p}\notin K$，$\Phi=a_0+a_1\phi^{1/p}+\cdots+a_{p-1}\phi^{(p-1)/p}=0$ $(a_i\in K,\ i=0,\cdots,p-1)$ とする。すると，$a_i=0$ $(i=0,\cdots,p-1)$ がなりたつ。

証明。 $F(X)=a_0+a_1X+\cdots+a_{p-1}X^{p-1}$，$G(X)=X^p-\phi$ とおいて $F(X)$ が恒等的に 0 でないとする。前に注意したように $F(X)$，$G(X)$ にユークリッドの互除法が行なえる。これによって得られ最大公約数を $Q(X)$ とすると，$Q(X)$ は K の元を係数にもつ X の整式で
$F(X)=Q(X)F_1(X)$, $G(X)=Q(X)G_1(X)$
と表わされる。ここで $F_1(X)$，$G_1(X)$ は K の元を係数にもつ整式で互いに素（すなわち $F_1(X)$ と $G_1(X)$ の最大公約数は 0 でない定数＝K の元）である。$Q(X)$ の X についての次数を α とする。もし α が正ならば $G(X)=X^p-\phi=0$ の根は $\phi^{1/p}$，$\varepsilon\phi^{1/p}$，$\cdots$，$\varepsilon^{p-1}\phi^{1/p}$ の p 個であるから $Q(X)=0$ の根は α 個で
$\varepsilon^{m_1}\phi^{1/p}$，$\varepsilon^{m_2}\phi^{1/p}$，$\cdots$，$\varepsilon^{m_\alpha}\phi^{1/p}$
$(0\leq m_1<\cdots<m_\alpha<p)$
と表わせる。ゆえに $Q(X)$ は
$Q(X)=c(X-\varepsilon^{m_1}\phi^{1/p})$
$\cdots(X-\varepsilon^{m_\alpha}\phi^{1/p})$ $(c\in K)$
と表わせる[2]。とくに $Q(X)$ の定数項は
$c(-1)^\alpha\varepsilon^m\phi^{\alpha/p}\neq 0$ $(m=m_1+\cdots+m_\alpha)$
であってこれは K の元である。K は複素数を含むから，$c(-1)^\alpha\varepsilon^m\in K$。ゆえ $\phi^{\alpha/p}\in K$ を得る。仮定より，$\alpha\leqq\deg F(X)\leqq p-1$ ゆえ α と p は互いに素な整数である。ゆえ、$\lambda\alpha+\nu p=1$ なる整数 λ，ν が存在する。ゆえに
$K\ni(\phi^{\alpha/p})^\lambda=\phi^{\alpha\lambda/p}=\phi^{(1-\lambda p)/p}=\phi^{1/p}\phi^{-\nu}$
がなりたつ。仮定より $\phi\in K$。ゆえ $\phi^\nu\in K$。ゆえに
$\phi^{1/p}=(\phi^{1/p}\phi^{-\nu})\phi^\nu\in K$
となりこれは補題の仮定に矛盾する。ゆえに $\alpha=0$，すなわち $Q(X)$ は 0 でない定数である。ゆえ $Q(X)=d\in K$ とおくと，再び前に述べたユークリッドの互除法より
$P(X)F(X)+R(X)G(X)=d\neq 0$
をみたす，K の元を係数とする整式 $P(X)$，$R(X)$ が存在する。補題の仮定より $F(\phi^{1/p})=0$，$G(\phi^{1/p})=0$ であるから上の式に $\phi^{1/p}$ を代入して
$0=P(\phi^{1/p})F(\phi^{1/p})+R(\phi^{1/p})G(\phi^{1/p})=d$
を得るがこれは矛盾である。ゆえ $F(X)$ は恒等的に 0 である。これは $a_i=0$ $(i=0,\cdots,p-1)$ に他ならない。 （証明終）

この補題を用いて（8）の主張を示すことは簡単である。すなわち条件より
$(a_0-b_0)+(a_1-b_1)\phi^{1/p}+$
$\cdots+(a_{p-1}-b_{p-1})\phi^{(p-1)/p}=0$
がなりたつ。そこで $a_i-b_i\in K$ であることに注意すれば補題が適用できて，$a_i-b_i=0$ $(i=0,\cdots,p-1)$ が得られる。

以上の結果をまとめると次のようになる。

（3．I） 複素数を係数にもつ有理式の集合，$K=\boldsymbol{C}(X_1,\cdots,X_5)$ は四則が可能，すなわち体である。

（3．II） p を素数，ϕ を K の任意の元とし $\phi^{1/p}$ を方程式 $X^p-\phi=0$ の一つの根とする。この $\phi^{1/p}$ について
$a_0+a_1\phi^{1/p}+\cdots+a_{p-1}\phi^{(p-1)/p}$
$(a_i\in K,\ i=0,\cdots,p-1)$
なる形の元の集合を $\boldsymbol{C}(X_1,\cdots,X_5,\ \phi^{1/p})$ 又は $K(\phi^{1/p})$ で表わすと $K(\phi^{1/p})$ は K を含み再び四則が可能な集合（体）である。

（3．Ⅲ）　$\phi^{1/p}\notin K$とする。$K(\phi^{1/p})$の中の2つの元Φ，Ψが

$$\Phi=a_0+a_1\phi^{1/p}+\cdots+a_{p-1}\phi^{(p-1)/p}$$

$$\Psi=b_0+b_1\phi^{1/p}+\cdots+b_{p-1}\phi^{(p-1)/p}$$

$$(a_i, b_i\in K,\ i=0,\cdots,p-1)$$

と表わされているとき

$$\Phi=\Psi\Leftrightarrow a_i=b_i\ (i=0,\cdots,p-1)$$

がなりたつ

4．有理式を含む体の列

$K(\phi^{1/p})$を前節で定義した四則可能な集合(体)とする。新たな素数q（p＝qでもよい）と$K(\phi^{1/p})$の任意の元ϕを考える。ゆえϕは

$$\phi=a_0+a_1\phi^{1/p}+\cdots+a_{p-1}\phi^{(p-1)/p}$$

$$(a_i\in K,\ i=0,\cdots,p-1)$$

なる形で表わされていることに注意する。$\phi^{1/q}$をϕの1つのq乗根とし

$$b_0+b_1\phi^{1/q}+\cdots+b_{q-1}\phi^{(q-1)/q}$$

$$(b_i\in K(\phi^{1/p}),\ i=0,\cdots,q-1)$$

なる形の元全体の集合を

$C(X_1,\cdots,X_5,\phi^{1/p},\phi^{1/q})$又は$K(\phi^{1/p},\phi^{1/q})$で表わす。この集合について次のことがなりたつ。

（4．Ⅰ）$K(\phi^{1/p})$は四則が可能，すなわち体，である。

（4．Ⅱ）$K(\phi^{1/p},\phi^{1/q})$は再び四則が可能な集合(体)で$K(\phi^{1/p})$を部分集合として含んでいる。

（4．Ⅲ）$\phi^{1/q}\notin K(\phi^{1/p})$とする。$K(\phi^{1/p},\phi^{1/q})$の中の2つの元$\Phi$，$\Psi$が

$$\Phi=b_0+b_1\phi^{1/q}+\cdots+b_{p-1}\phi^{(q-1)/q}$$

$$\Psi=c_0+c_1\phi^{1/q}+\cdots+c_{p-1}\phi^{(q-1)/q}$$

$$(b_i, c_i\in K(\phi^{1/p}),\ i=0,\cdots,q-1)$$

とすると

$$\Phi=\Psi\Leftrightarrow b_i=c_i\ (i=0,\cdots,q-1)$$

がなりたつ。

（4．Ⅰ）は前節で示した。（3．Ⅱ）及び（3．Ⅲ）の証明中Kについて用いている条件はKが四則可能すなわち体，ということだけである。それゆえ（4．Ⅱ）及び（4．Ⅲ）については，（3．Ⅱ）及び（3．Ⅲ）の証明においてK，p，ϕをそれぞれ$K(\phi^{1/p})$，q，ϕにおきかえてもまったく同様に証明できる。このようにして四則の可能な集合の有限列

$$K\subset K(\phi^{1/p})\subset K(\phi^{1/p},\phi^{1/q})\subset K(\phi^{1/p},\phi^{1/q},\delta^{1/r})\subset\cdots$$

を定義することができる。便宜上

$$\phi^{1/p}=\Phi_1,\quad \phi^{1/q}=\Phi_2,\quad \delta^{1/r}=\Phi_3,\cdots$$

$$p=p_1,\quad q=p_2,\quad r=p_3,\cdots$$

とおくと上の列は

$$K\subset K(\Phi_1)\subset K(\Phi_1,\Phi_2)\subset\cdots\subset K(\Phi_1,\cdots,\Phi_n)$$

と表わされて次の性質（P_1），（P_2），（P_3）をみたす。

（P_1）Kは体である。

（P_2）素数 p_1，$p_2,\cdots$，p_n について

$$\Phi_i^{p_i}\in K(\Phi_1,\cdots,\Phi_{i-1})\ (i=1,\cdots,n)$$

がなりたち，$K(\Phi_1,\cdots,\Phi_i)$の任意の元は

$$a_0+a_1\Phi_2+\cdots+a_\lambda\Phi_i^\lambda$$

$$(\lambda=p_i-1,\ a_j\in K(\Phi_1,\cdots,\Phi_{i-1}),\ j=0,\cdots,p_i-1)$$

と表わせる。ここでi＝0のときは，$K=K(\Phi_1,\cdots,\Phi_{i-1})$としておく。

（P_3）$\Phi_i\notin K(\Phi_1,\cdots,\Phi_{i-1})$とする。$K(\Phi_1,\cdots,\Phi_i)$の元$\Phi$，$\Psi$について

$$\Phi=a_0+a_1\Phi_i+\cdots+a_\lambda\Phi_i^\lambda$$

$$\Psi=b_0+b_1\Phi_i+\cdots+b_\lambda\Phi_i^\lambda$$

$$(\lambda=p_i-1,\ a_j, b_j\in K(\Phi_1,\cdots,\Phi_{i-1}),\ j=0,\cdots,p_i-1)$$

とすると

$$\Phi=\Psi\Leftrightarrow a_j=b_j\ (j=0,\cdots,p_i-1)$$

がなりたつ。

上のKについては$K=C(X_1,\cdots,X_5)$について考えているが変数の個数mを任意にとって$K=C(X_1,\cdots,X_m)$としてもまったく同様である。とくに$K=C(X_1,X_2,X_3)$としても同様の議論がなりたつ。

5．代数的解法の定義

以下5次方程式の代数的解法は不可能であることの意味を説明する。そのためにはまず5次方程式の代数的解法とはいかなることであるかを明確にしておく必要がある。

そこで最初に例として，3次方程式について考えてみょう。Δ，A，Bを2節で定義したものと

し，$\Phi_1=\Delta$，$\Phi_2=A$，$\Phi_3=B$とおく。更に$K=C(X_1, X_2, X_3)$[3]とすると，2節で示したように

$$x_i \in K(\Phi_1, \Phi_2, \Phi_3) \quad (i=1, 2, 3)$$

がなりたつ。又

$$\Phi_2^2 \in K, \quad \Phi_3^2 \in K(\Phi_1), \quad \Phi_3^3 \in K(\Phi_1, \Phi_2)$$

がなりたつから（P_1），（P_2）をみたす。すなわち3次方程式の根の公式を求めるということは上のKに対してΦ_1，$\Phi_2, \cdots, \Phi_n$を求めて

$$x_i \in K(\Phi_1, \Phi_2, \cdots, \Phi_n) \quad (i=1, 2, 3)$$

かつΦ_j（$j=1, \cdots, n$）が（P_1），（P_2）をみたすようにすることであった。

次に5次方程式について考える。まず5次方程式とは一般的には

$$a_0X^5+a_1X^4+a_2X^3+a_3X^2+a_4X+a_5=0 \quad (a_0 \neq 0)$$

なる形の方程式であるが，根の公式を考える場合2次又は3次の場合と同様，特に$a_0=1$の場合のみを考えればよい。この方程式の根をx_1，x_2，x_3，x_4，x_5とすれば根と係数の関係から

$$\begin{aligned} -a_1 &= x_1+x_2+\cdots+x_5 \\ a_2 &= x_1x_2+\cdots+x_4x_5 \\ -a_3 &= x_1x_2x_3+\cdots+x_3x_4x_5 \\ a_4 &= x_1x_2x_3x_4+\cdots+x_2x_3x_4x_5 \\ -a_5 &= x_1x_2x_3x_4x_5 \end{aligned}$$

と表わせる。そこで$X_1, \cdots, X_5$を$X_1, \cdots, X_5$の1次，$\cdots$，5次の基本対称式とすれば$a_i=(-1)^iX_i$（$i=1, \cdots, 5$）がなりたつ。そこでこの5次方程式の代数的解法とは$X_1, \cdots, X_5$を$X_1, \cdots, X_5$とベキ根を用いて表わすことである。すなわち根の公式（又は代数的解法）があるということは，$K=C(X_1, \cdots, X_5)$とおいたとき（P_1），（P_2）をみたすΦ_i（$i=1, \cdots, n$）が存在して$x_j \in K(\Phi_1, \cdots, \Phi_n)$（$j=1, \cdots, 5$）と定義するのである。

（注．代数的解法において現在考えているのは素数次のベキ根のみを取り扱っているが，素数次以外のベキ根は素数次のベキ根で表わすことができる。たとえばある数Eの4乗根$E^{1/4}$は2乗根を2回用いて，$E^{1/4}=(E^{1/2})^{1/2}$と表わせる。6乗根は，$E^{1/6}=(E^{1/2})^{1/3}$と考える。このようにして素数乗根のみを考えればよいことがわかる。）

簡単な例によって上に述べたことを確かめてみよう。たとえば仮に

$$X_1=(X_1+(X_2^2+X_3X_4)^{1/2})^{1/3}/(X_2+(X_3X_5+X_2^3)^{1/4})^{1/5}$$

と表わせるとする。この場合は

$$\Phi_1=(X_2^2+X_3X_4)^{1/2}, \quad \Phi_2=(X_3X_5-X_2^3)^{1/2},$$
$$\Phi_3=(X_3X_5-X_2^3)^{1/4}, \quad \Phi_4=(X_1+\Phi_1)^{1/3}$$
$$\Phi_5=(X_2+\Phi_3)^{1/5}$$

とおけば，$\Phi_1, \cdots, \Phi_5$は（P_1），（P_2）をみたし$X_1 \in K(\Phi_1, \cdots, \Phi_5)$である。

次の補題はルフィニによって予想され，アーベルによって証明されたもので代数方程式論の要である。

補題．X_i（$i=1, \cdots, 5$）は不定元$x_1, \cdots, x_5$のi次の基本対称式とし，$K=C(X_1, \cdots, X_5)$とおく。（P_1），（P_2）をみたす$\Phi_1, \cdots, \Phi_n$が存在して

$$x_1, \cdots, x_5 \in K(\Phi_1, \cdots, \Phi_n)$$

とできるならば，$\Phi_1, \cdots, \Phi_n$をうまく選ぶことによって$\Phi_1, \cdots, \Phi_n$を$x_1, \cdots, x_5$の有理式（複素数係数）とすることができる。

この補題により5次方程式に根の公式が存在すると仮定すると，その公式に表われるベキ根は$x_1, \cdots, x_5$の複素数を係数とする有理式で表わされることがわかる。

証明は後にまわし，当面この補題の成立を仮定して議論を進める。

6．根の置換

$x_1, \cdots, x_5$を不定元とし$F=F(x_1, \cdots, x_5)$を有理式とする。{1，2，3，4，5}の任意の置換σについて

$${}^{\sigma}F=F(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}, x_{\sigma(5)})$$

で，${}^{\sigma}F$を定義する。τを{1，2，3，4，5}のもう一つの任意の置換とするとその積$\sigma\tau$について容易に${}^{(\sigma\tau)}F={}^{\sigma}({}^{\tau}F)$が確かめられる。ゆえ${}^{\sigma\tau}F$で表わしても誤解は生じない。

たとえば

$$\sigma=\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}, \quad \tau=\begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix}$$

とすると

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\4&5&3&1&2\end{pmatrix}$$

である。ゆえに

$$^{(\sigma\tau)}F = F(x_4, x_5, x_3, x_1, x_2)$$

である。一方 $^{\tau}F = G$ とおくと

$$G = G(x_1, x_2, x_3, x_4, x_5) = F(x_5, x_4, x_1, x_2, x_3)$$

であるから

$$^{\sigma}(^{\tau}F) = {}^{\sigma}G = G(x_3, x_1, x_2, x_5, x_4) = F(x_4, x_5, x_3, x_1, x_2) = {}^{(\sigma\tau)}F$$

がなりたつ。

さて

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5) \times (x_2 - x_3)(x_2 - x_4)(x_2 - x_5) \times (x_3 - x_4)(x_3 - x_5) \times (x_4 - x_5)$$

を差積とする。すると σ が偶置換のとき $^{\sigma}\Delta = \Delta$，奇置換のとき $^{\sigma}\Delta = -\Delta$ がなりたつことに注意する。Δ のように任意の奇置換 σ について $^{\sigma}F = -F$ なる有理式を交代有理式という。

補題. $F = F(x_1, \cdots, x_5)$ を対称式でない整式で，F^2 は対称式であるとする。すると $F = G\Delta$ と表わせる。ここで G は対称式である。

証明. F は対称式でないからある互換 σ に対して $^{\sigma}F \neq F$ となる。$\sigma = (1\ 2)$ としてよい。

$$^{\sigma}(F^2) = (^{\sigma}F)^2$$

がなりたつから

$$(^{\sigma}F)^2 = F^2$$

がなりたつ。すなわち $^{\sigma}F = \pm F$ のどちらかであるが $^{\sigma}F \neq F$ という仮定より $^{\sigma}F = -F$ である。つまり，$^{\sigma}F + F = 0$ がなりたつ。すなわち

$$F(x_2, x_1, x_3, x_4, x_5) + F(x_1, x_2, x_3, x_4, x_5) = 0$$

これに $x_1 = x_2$ を代入して

$$2F(x_2, x_2 x_3, x_4, x_5) = 0$$

ゆえ剰余定理より F は $x_1 - x_2$ で割り切れる。ゆえに

$$F = (x_1 - x_2)^m F_1 \quad (m > 0)$$

と表わされ，F_1 は $x_1 - x_2$ で割り切れない整式である。

仮定によって

$$F^2 = (x_1 - x_2)^{2m} F_1^2$$

は対称式である。ゆえ任意の相異なる i，j（$i, j = 1, \cdots, 5$）について $\tau(1) = i$，$\tau(2) = j$ なる置換 τ を考えれば

$$F^2 = {}^{\tau}(F^2) = (x_i - x_j)^{2m}\ {}^{\tau}(F_1^2)$$

がなりたつ。ゆえに

$$F = \pm (x_i - x_j)^m\ {}^{\tau}(F_1)$$

のどちらかである。結局任意の $i \neq j$（$i, j = 1, \cdots, 5$）について，F は $(x_i - x_j)^m$ で割り切れるから，Δ^m でも割り切れる。すなわち

$$F = \Delta^m F_2$$

と表わせる。ここで F_2 は整式である。

F_2 が $x_i - x_j$（$i \neq j$）で割り切れないことを示そう。もし F_2 が $x_i - x_j$ で割り切れるとすると F は $(x_i - x_j)^{m+1}$ で割り切れる。ゆえに F^2 は $(x_i - x_j)^{2m+2}$ で割り切れる。すなわち

$$F^2 = (x_i - x_j)^{2m+2} F_3^2$$

と表わせる。F_3 は整式である。そこで ρ を $\rho(i) = 1$，$\rho(j) = 2$ なる置換，たとえば $\rho = \tau^{-1}$，とすれば

$$F^2 = {}^{\rho}(F^2) = (x_1 - x_2)^{2m+1}\ {}^{\rho}(F_3^2)。$$

ゆえに F は $(x_1 - x_2)^{m+1}$ で割り切れる。ゆえ F_1 が $x_1 - x_2$ で割り切れることになって矛盾が生ずる。

次に F_2 が対称式であることを示す。

$$F^2 = \Delta^{2m} F_2^2$$

で，F^2，Δ^{2m} は両方とも対称式であるから F_2^2 も対称式。ゆえ F_2 が対称式でないとすると F_2 に対して F の場合と同様な議論が適用できて，F_2 は $x_1 - x_2$ で割る切れる。これは F_2 の仮定に矛盾する。ゆえ F_2 は対称式である。

最後に m が偶数であるとすると Δ^m は対称式，ゆえ F も対称式となり補題の仮定に反する。ゆえ m は奇数である。$m = 2r + 1$ と表わして

$$G = \Delta^{2r} F_2$$

とおけばこれが求める対称式である。（証明終）

系1. $F = F(x_1, \cdots, x_5)$ は任意の偶置換 σ について $^{\sigma}F = F$ なる整式とする。すると

$$F = F_1 + F_2\Delta \quad (F_i \text{は対称式}, i = 1, 2)$$

と表わせる。

証明. τ を任意の奇置換，α を互換（1 2）とする。すると $\alpha\tau$ は偶置換となるから仮定により

$$^{\alpha\tau}F = F$$

がなりたつ。ゆえに

$$^{\tau}F = {}^{\alpha\alpha^{\tau}}F = {}^{\alpha}F$$

である。このことよりF＋$^{\alpha}$Fは対称式であることがわかる。なぜならばβを任意の互換とすると

$$^{\beta}(F + {}^{\alpha}F) = {}^{\beta}F + {}^{\beta\alpha}F = {}^{\beta}F + F$$

又上で述べたことから $^{\beta}F = {}^{\alpha}F$。ゆえ

$$^{\beta}(F + {}^{\alpha}F) = {}^{\alpha}F + F$$

がなりたつ。

他方F－$^{\alpha}$Fは交代式である。すなわち任意の互換βについて

$$^{\beta}(F - {}^{\alpha}F) = {}^{\beta}F - {}^{\beta\alpha}F = {}^{\beta}F - F。$$

上と同様にして

$$^{\beta}(F - {}^{\alpha}F) = {}^{\alpha}F - F$$

を得る。交代式の2乗は対称式であるから前の補題を利用して

$$F - {}^{\alpha}F = 2F_2\Delta \quad (F_2は対称式)$$

と表わせる。ゆえに

$$F + {}^{\alpha}F = 2F_1$$

とすれば

$$F = F_1 + F_2\Delta \quad (F_1, F_2は対称式)$$

となる。　　（証明終）

Fが有理対称式とは，Fは有理式であってかつ任意の互換σについて$^{\sigma}F = F$をみたすものである。

有理対称式は対称式の商で表わせることは次のようにして示すことができる。

まずFが有理式であるとき，F＝L／H（L，H は整式でH≠0）と表わせる。{1，2，3，4，5} の置換の個数は5！＝120であることに注意して，それらの置換をσ_1，σ_2，σ_3，…，σ_{120}とする。ここでσ_1は恒等置換としておく，そこで

$$H_i = {}^{\sigma_i}H \quad (\sigma = \sigma_i,\ i = 1, \cdots, 120)$$

とおく。すると任意の互換τについて

$$^{\tau}(H_1H_2\cdots H_{120}) = H_1H_2\cdots H_{120}$$

がなりたつ。なぜならτば

$$\tau\sigma_i = \tau\sigma_j \Leftrightarrow \sigma_i = \sigma_j \Leftrightarrow i = j$$

がなりたつから

$$\tau\sigma_1,\ \tau\sigma_2, \cdots, \tau\sigma_{120}$$

はすべて互いに相異なる元となる。ゆえ上記の$\tau\sigma_i$（i＝1，…，120）はすべて置換を表わしている。すなわち集合として

$$\{\sigma_1, \cdots, \sigma_{120}\}$$

と

$$\{\tau\sigma_1, \cdots, \tau\sigma_{120}\}$$

は等しい。ゆえに

$$\begin{aligned} ^{\tau}(H_1H_2\cdots H_{120}) &= {}^{\tau}({}^{\alpha}H\,{}^{\beta}H\cdots{}^{\gamma}H) \\ &= {}^{\tau\alpha}H\,{}^{\tau\beta}H\cdots{}^{\tau\gamma}H \\ &= {}^{\alpha}H\,{}^{\beta}H\cdots{}^{\gamma}H \\ &= H_1H_2\cdots H_{120} \end{aligned}$$

$$(\alpha = \sigma_1,\ \beta = \sigma_2,\ \cdots,\ \gamma = \sigma_{120})$$

がなりたつ。このことは$H_1H_2\cdots H_{120}$が対称式であることを意味する。

さてH＝H_1に注意すれば

$$F = LH_2\cdots H_{120} / H_1H_2\cdots H_{120}$$

であるから

$$LH_2\cdots H_{120} = FH_1H_2\cdots H_{120}$$

ゆえ任意の互換τに対して$^{\tau}F = F$に注意すれば

$$\begin{aligned} ^{\tau}(LH_2\cdots H_{120}) &= {}^{\tau}(FH_1H_2\cdots H_{120}) \\ &= {}^{\tau}F\,{}^{\tau}(H_1H_2\cdots H_{120}) \\ &= FH_1H_2\cdots H_{120} \end{aligned}$$

であるから$LH_2\cdots H_{120}$は対称式である。

そこをあらためてHを$H_1H_2\cdots H_{120}$，，Lを$LH_2\cdots H_{120}$とおけばよい。

上記の証明では対称式としてF＝L／HのLとHを選ぶときLとHに共通の定数以外の因数（すなわち公約数）が存在する。実はL，Hにはこのような公約数が存在しないように選ぶことができるがその証明には5変数の複素数係数をもつ整式の一意分解性が必要であると思われる（一意分解性を用いない証明を著者は知らない）。それには環の議論が必要であり，本論文の主旨に反する上，そこまでの条件をここでは要求しない。

系2．　F＝F(X_1，…，X_5）を対称でない有理式で，F^2は対称であるとする。すると有理対称式Gが存在してF＝GΔと表わせる。

証明．　F＝L／H（L，Hは整式，H≠0）とする。H_1，H_2，…，H_{120}を上記のものとすると

$$F = LH_2\cdots H_{120} / H_1H_2\cdots H_{120}$$

であるから，あらためてL＝$LH_2\cdots H_{120}$，H＝$H_1H_2\cdots H_{120}$とおくことにより始めからHは対称式としてよい。仮定より$F^2 = L^2 / H^2$は対称有理式であるから，前証明と同様にしてL^2は対称式である。そこでLがもし対称式ならばFは対称になって仮定に矛盾する。ゆえにLに対して補題が適用できてL＝MΔ（Mは対称式）と表わ

せる。ゆえにG＝M／Hとおけば G は有理対称式であってF＝GΔと表わせる。　　（証明終）

系3.　F＝F(x_1, •••, x_5) は任意の偶置換 σ について $^{\sigma}F = F$ なる有理式とする。すると

$$F = F_1 + F_2\Delta \quad (F_1, F_2 \text{は有理対称式})$$

と表わせる。

証明.　系1の場合とまったく同様に証明できる。この場合補題のかわりに系2を用いればよい。

（証明終）

以下代数方程式論（Ⅱ）へ続く。

参考文献

(1) N.H Abel, Beweis der Unmöglichkeit algebraiche Gleichungen von höheren Graden als dem vierten allgemein aufzulösen, Journal füs die reine und angewandte Mathematik, vol 1, (1826) 65－84.
(注). この日本語訳と現代代数学の立場からの解説が，守屋美賀雄　訳，解説　アーベル，ガロア　群と代数方程式＜現代数学の系譜11＞(1975) 共立出版にでている。

(2) 淡中忠郎，代数学（1964）朝倉書店。

注

1）次に示さている補題を $\varepsilon^i \phi^{1/p}$ (i ＝ 1, •••, p － 1) に適用すると，$F(\phi^{1/p}) \neq 0$ より $F(\varepsilon^i \phi^{1/p}) \neq 0$ を得るゆえ $G' \neq 0$ である。

2）ε^{m_1}, ε^{m_2}, •••, ε^{m_a} はそれぞれ ε の m_1 乗，m_2 乗，•••，m_a 乗を表わしている。

3）x_1, x_2, x_3 を不定元とみて $-a = X_1$, $b = X_2$, $-c = X_3$ とおく。