広島大学附属中・高等学校研究紀要
〈第49号　2002〉

「5次以上の代数方程式は一般に巾根では解けないことの証明」について
――高校生を対象としたアーベルの定理の講義――

河　野　芳　文

本稿は，私が本校高等学校数学研究班の生徒の求めに応じて行った代数方程式に関するアーベルの定理「5次以上の代数方程式は，一般に巾根では解けない」についての証明の講義録と，実施した結果の問題点や反省についての報告からなる。中学校から高等学校にかけて，1次方程式，2次方程式の解の公式を学び，数学Bで高次方程式について学んだ生徒が，3次以上の方程式の解の公式に興味をもつのは自然であり，解の公式が無い理由を知りたいと欲する気持ちを尊重したいと考えて行った講義である。高校生が持つ知識や論理的思考力を考えて，予備知識の少ない高木貞治著「代数学講義」の流儀に沿う形で，方程式解法の歴史，4次以下の方程式の解法，置換群と多項式，本定理の証明となっているが，アーベル生誕200年の年である2002年にこのような講義ができた偶然を幸いと思う。

1. はじめに

方程式の理論の歴史は，紀元前1500年頃の古代バビロニアの2次方程式の解法にまで遡ることができる。しかし，バビロニアの人々はそれを記述する代数的記号を持っていない上，負の数の考えもなかったため，今日のように整理された扱いにはなっていない。古代ギリシア人も2次方程式を幾何学的作図によって解いているが，少なくとも西暦100年頃までは代数的な定式化は存在しなかったと考えられている。

その後しばらくは大きな進歩も見られなかったが，ルネッサンス期のイタリア，ボロニアの数学者達が3次方程式の解法について熱心に取り組み，デル・フェロ，フォンタナ（タルタリア）が3次方程式の解法を発見している（16世紀前半）。このタルタリアから解法を教わったカルダノは，自分の弟子フェラリが発見した4次方程式の解法も含めて，著書「アルス・マグナ」で公にするが，代数的記号法は，16世紀後半のヴィエタ，17世紀前半のデカルトにいたってようやく完成した。

こうした流れの中にあって，次に目標としたものは5次方程式の解法であったが，チルンハウス，ライプニッツ，オイラー，ラグランジュの試みにも関わらず，その解法を発見することはできなかった。しかし，1770年のラグランジュによる4次以下の方程式についての統一された考察は，方程式の可解性が方程式の根にいくつかの置換を施したときに不変となる関数を見い出すことに帰着することを示したが，その方法は5次方程式には適用できないことをも示した。

その後，5次方程式は巾根では解けないのではとの雰囲気が広まり，ルフィニは1813年に不可能性の証明を発表した。しかし，その証明にはいくつかの欠陥があったため，1824年の有名なアーベルの論文をもって最終的な解決をみた。

現代においては，方程式の理論は一般的な体論の中で触れられるのが普通であるが，高校生を相手とした講義であるから，以下における展開は予備知識の少ない高木貞治著「代数学講義」に近い方法をとり，必要な事柄を追加して説明する形をとった。

2. 4次以下の代数方程式の解法

代数方程式 $a_0x^n+a_1x^{n-1}+\cdots+a_n=0$ は，最高次の係数で両辺を割ることにより，初めから $a_0=1$ と考えてよい。(a_i：複素数)

1）1次方程式 $x+a_1=0$

解は，$x=-a_1$

2）2次方程式 $x^2+a_1x+a_2=0$

$$\left(x+\frac{a_1}{2}\right)^2-\frac{a_1^2}{4}+a_2=0 \text{ より，}$$

$$\left(x+\frac{a_1}{2}\right)^2=\frac{a_1^2-4a_2}{4}$$

両辺の平方根をとって

$$x+\frac{a_1}{2}=\pm\frac{\sqrt{a_1^2-4a_2}}{2}$$

これより，求める解は，

$$x=\frac{-a_1\pm\sqrt{a_1^2-4a_2}}{2}$$

On the Proof of Unsolvability of Algebraic Equations of Degree n ($n \geqq 5$)
—— Lectures in Senior High School ——
Yoshifumi KOHNO

3） 3次方程式 $x^3+a_1x^2+a_2x+a_3=0$

$y=x+\frac{a_1}{3}$ とおけば，$x=y-\frac{a_1}{3}$ であるから，

$$\left(y-\frac{a_1}{3}\right)^3+a_1\left(y-\frac{a_1}{3}\right)^2+a_2\left(y-\frac{a_1}{3}\right)+a_3=0$$

$$y^3+\frac{3a_2-a_1^2}{3}y+\left(a_3+\frac{2}{27}a_1^3-\frac{a_1a_2}{3}\right)=0$$

従って，$X^3+aX+b=0$ の形の方程式が解ければよい。

今，$X=Y-\frac{a}{3Y}$ とおくと，

$$\left(Y-\frac{a}{3Y}\right)^3+a\left(Y-\frac{a}{3Y}\right)+b=0$$

$$Y^3+b-\frac{a^3}{27Y^3}=0$$

$$27(Y^3)^2+27bY^3-a^3=0$$

2次方程式の解の公式より，

$$Y^3=\frac{-27b\pm\sqrt{(27b)^2+108a^3}}{54}=\frac{-b\pm\sqrt{b^2+\frac{4}{27}a^3}}{2}$$

$R=b^2+\frac{4}{27}a^3$ とおいて，$u=\sqrt[3]{\frac{-b+\sqrt{R}}{2}}$，

$v=\sqrt[3]{\frac{-b-\sqrt{R}}{2}}$ を考えると，u, v ともに3通りの根がある。これら6つの Y の値に対して $X=Y-\frac{a}{3Y}$ の値を求めると，2つずつ同じ値となり，方程式 $X^3+aX+b=0$ の3つの解を得る。

なお，1つの u に対して $x=u-\frac{a}{3u}$ とおくと，

$$3u^2-3xu-a=0$$

よって，2次方程式 $3t^2-3xt-a=0$ の解を u, u' とすると，

$$u+u'=x,\ uu'=-\frac{a}{3}$$

であり，

$$u^3+(u')^3=(u+u')^3-3uu'(u+u')=x^3+ax=-b$$

$$u^3(u')^3=(uu')^3=-\frac{a^3}{27}$$

これは，u^3, $(u')^3$ が2次方程式

$$27t^2+27bt-a^3=0$$

の解であること，したがって，u' がある v に一致することを示す。

よって，$x=u+v$ とかける。こうして1組の解が得られると，他の解は，ω を1の立方根として，

$$\omega u+\omega^2 v,\ \omega^2 u+\omega v$$

で与えられることが分かる。

4） 4次方程式 $x^4+a_1x^3+a_2x^2+a_3x+a_4=0$

$y=x+\frac{a_1}{4}$ とおくと，

$$\left(y-\frac{a_1}{4}\right)^4+a_1\left(y-\frac{a_1}{4}\right)^3+a_2\left(y-\frac{a_1}{4}\right)^2+a_3\left(y-\frac{a_1}{4}\right)+a_4=0$$

これを展開して整理すると，

$$y^4+\left(a_2-\frac{3}{8}a_1^2\right)y^2+\left(\frac{1}{8}a_1^3-\frac{1}{2}a_1a_2+a_3\right)y+\left(\frac{-3}{256}a_1^4+\frac{1}{16}a_1^2a_2-\frac{1}{4}a_1a_3+a_4\right)=0$$

従って，次の形の4次方程式が解ければよい。

$$X^4+aX^2+bX+c=0$$

$X^4=-aX^2-bX-c$ の両辺に $yX^2+\frac{1}{4}y^2$ を加えて，

$$\left(X^2+\frac{1}{2}y\right)^2=(y-a)X^2-bX+\left(\frac{1}{4}y^2-c\right)\quad\text{—(1)}$$

右辺が X についての完全平方式となる条件を求めると，

$D=b^2-(y-a)(y^2-4c)=0$，すなわち

$$y^3-ay^2-4cy+4ac-b^2=0\quad\text{————(*)}$$

この y の3次方程式の1つの根を求めて(1)に代入すると，

$$\left(X^2+\frac{1}{2}y\right)^2=(y-a)\left(X-\frac{b}{2(y-a)}\right)^2$$

$$\therefore\ X^2+\frac{1}{2}y=\sqrt{y-a}\left(X-\frac{b}{2(y-a)}\right)$$

または，$-\sqrt{y-a}\left(X-\frac{b}{2(y-a)}\right)$

これらを X について解いて，X の4つの値を求めることができる。（方程式(*)の他の根 y を用いても同一の解を得る。）

3. 置換群と対称式・交代式

まず，置換について述べよう。

定義：相異なる n 個のものを，1つの順序から他の順序に置きかえることを置換という。置換を σ, τ, ρ … などで表し，n 個のものの置換全体を S_n で表す。また，便宜上 n 個のものに番号をつけて 1, 2, …, n で表し，置換 σ によって順序1，2，…，n が順序 a_1, a_2, …, a_n に変わることを，$\sigma=\begin{pmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{pmatrix}$ と記す。あるいは，$a_i=\sigma(i)$ とおき，$\sigma=\begin{pmatrix}1&2&\cdots&n\\\sigma(1)&\sigma(2)&\cdots&\sigma(n)\end{pmatrix}$ と記す。

(注) たとえば，S_3 において，$\sigma=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ は 1，2，3 を 3，1，2 の順序にすることを表すが，上の行の数 p が "p 番目" を表し，その下の数 q が "p 番目の数が q" となることを意味すると考えて，

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

と表してもよいことにする。

定義：置換 $\sigma=\begin{pmatrix}1&2&\cdots&n\\\sigma(1)&\sigma(2)&\cdots&\sigma(n)\end{pmatrix}$ に対し，$\sigma^{-1}=\begin{pmatrix}\sigma(1)&\sigma(2)&\cdots&\sigma(n)\\1&2&&n\end{pmatrix}$ を σ の逆置換といい，何も動かさない置換 $1_n=\begin{pmatrix}1&2&\cdots&n\\1&2&\cdots&n\end{pmatrix}$ を恒等置換という。(1_n を単に 1 ともかく。)

(例 1) S_3 において，$\sigma=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ とすると，

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

$$1_3=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

定義：置換 $\sigma\in S_n$ を，i を $\sigma(i)$ に対応させる集合 $\{1,2,\cdots,n\}$ からそれ自身への関数とみる。σ，$\tau\in S_n$ に対し，$\sigma(i)$ を τ で写した像を $\tau(\sigma(i))$ で表し，置換

$$\begin{pmatrix}1&2&\cdots&n\\\tau(\sigma(1))&\tau(\sigma(2))&\cdots&\tau(\sigma(n))\end{pmatrix}$$

を，σ と τ の合成といって，$\tau\circ\sigma$ で表す。

$\tau\circ\sigma$ も n 個のものの置換であるが，一般に，$\tau\circ\sigma\neq\sigma\circ\tau$ である。

(例 2) $\sigma=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$，$\tau=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ のとき，

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

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

定理 1　1) $n(S_n)=n!$

2) σ，τ，$\rho\in S_n$ とすると，

i) $\rho\circ(\tau\circ\sigma)=(\rho\circ\tau)\circ\sigma$

ii) $\sigma^{-1}\circ\sigma=\sigma\circ\sigma^{-1}=1$

iii) $1\circ\sigma=\sigma\circ1=\sigma$

∵ 1) S_n は，異なる n 個のものの順列の全体であるから，その総数 $n(S_n)=n!$

2) i) σ によって i が j にうつされ，τ によって j が k にうつされ，ρ によって k が l にうつされるとすれば，

$\rho\circ(\tau\circ\sigma)(i)=\rho(k)=l$

$(\rho\circ\tau)\circ\sigma(i)=(\rho\circ\tau)(j)=l$

$\therefore\ \rho\circ(\tau\circ\sigma)=(\rho\circ\tau)\circ\sigma$

ii)

$$\sigma^{-1}\cdot\sigma=\begin{pmatrix}\sigma(1)&\sigma(2)&\cdots&\sigma(n)\\1&2&\cdots&n\end{pmatrix}\begin{pmatrix}1&2&\cdots&n\\\sigma(1)&\sigma(2)&\cdots&\sigma(n)\end{pmatrix}=\begin{pmatrix}1&2&\cdots&n\\1&2&\cdots&n\end{pmatrix}=1_n$$

$\sigma\circ\sigma^{-1}=1_n$ についても同様

iii) 明らか。

(例 3) $\sigma,\tau\in S_n$ のとき，$(\tau\circ\sigma)^{-1}=\sigma^{-1}\circ\tau^{-1}$

∵) $(\sigma^{-1}\circ\tau^{-1})\circ(\tau\circ\sigma)=\sigma^{-1}\circ(\tau^{-1}\circ\tau)\circ\sigma=\sigma^{-1}\circ1\circ\sigma=1_n$

$(\tau\circ\sigma)\circ(\sigma^{-1}\circ\tau^{-1})=\tau\circ(\sigma\circ\sigma^{-1})\circ\tau^{-1}=\tau\circ1\circ\tau^{-1}=1_n$

一方，$(\tau\circ\sigma)^{-1}\circ(\tau\circ\sigma)=(\tau\cdot\sigma)\circ(\tau\circ\sigma)^{-1}=1$ であるから，$(\sigma^{-1}\circ\tau^{-1})\circ(\tau\circ\sigma)=(\tau\circ\sigma)^{-1}\cdot(\tau\circ\sigma)$

両辺の右から $(\tau\circ\sigma)^{-1}$ を施して，

$\sigma^{-1}\circ\tau^{-1}=(\tau\circ\sigma)^{-1}$

(この証明は，置換 σ の逆置換がただ一通りに定まることの証明法をも示すものである。)

定義：置換 $\sigma\in S_n$ が，i を j に，j を k に，…，l を m に，m を i に置きかえる置換であるとき，σ を巡回置換といい，$\sigma=\begin{pmatrix}i&j&k&\cdots&m&x&\cdots&y\\j&k&\cdots&\cdots&i&x&\cdots&y\end{pmatrix}=(i\ j\ k\cdots m)$ と表す。特に，i と j のみを入れかえる巡回置換 $(i\ j)$ を互換という。

(例 4) $\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&4&1&6&5&2\end{pmatrix}\in S_6$ とすると，

$\sigma=(2\,4\,6)(1\,3)$

定理 2　1) 任意の置換は，同じ数字を含まない巡回置換の合成として表される。

2) 巡回置換は，いくつかの互換の合成として表すことができる。とくに，$(1a)$ の形の互換の合成として表すことができる。

∵ 1) $\sigma\in S_n$ について，1，$\sigma(1)$，$\sigma^2(1)$，… のうち，初めて重複するものを $\sigma^i(1)$ とし，$\sigma^j(1)=\sigma^i(1)$ $(0\leqq j<i)$ とすると，$1=\sigma^{i-j}(1)$ より，$i-j=i$ よって，$j=0$ で，$\sigma^i(1)=1$　次に，1，$\sigma(1)$，$\sigma^2(1)$，…，$\sigma^{i-1}(1)$ 以外の自然数 k をとり，k，$\sigma(k)$，$\sigma^2(k)$，… について同様のことを行う。以下同様にして，σ を巡回置換の合成

$\sigma=\big(1\ \sigma(1)\cdots\sigma^{i-1}(1)\big)\big(k\ \sigma(k)\cdots\sigma^{j-1}(k)\big)\cdots$

として表すことができる。残る部分の証明は容易。

2) $(ijk\cdots m)=(im)\cdots(i\,k)(i\,j)$，

$(ij)=(1i)(1j)(1i)$ より，明らか。

（例５）$(1\,3\,5\,4)\in S_5$とすると，

$$(1\,3\,5\,4)=\begin{pmatrix}3&2&5&4&1\\3&2&5&1&4\end{pmatrix}\begin{pmatrix}3&2&1&4&5\\3&2&5&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix}$$
$$=(1\,4)(1\,5)(1\,3)$$

定理３　任意の置換 $\sigma\in S_n$ を互換の合成として表すとき，合成する互換の個数の偶奇は σ のみにより，不変である。また，S_n の置換のうち，偶数個の互換の合成となるものを偶置換，奇数個の互換の合成となるものを奇置換と呼ぶ。偶置換の全体 A_n，奇置換の全体の個数は等しく，ともに $\dfrac{n!}{2}$ で与えられる。

∵ n 変数の文字 $x_1,\ x_2,\ \cdots,x_n$ に対し，異なる２文字の差 $x_i-x_j(i<j)$ 全体の積で与えられる多項式

$$\Delta(x_1,x_2,\cdots,x_n)=\prod_{i<j}(x_i-x_j)$$

を，$x_1,\ x_2,\cdots,x_n$ の差積という。今，$\sigma\in S_n$ に対して，

$$\sigma\big(\Delta(x_1,x_2,\cdots,x_n)\big)=\Delta(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)})$$

と定めると，右辺は $\pm\Delta(x_1,x_2,\cdots,x_n)$ のいずれかに等しい。とくに，σ が互換で $\sigma=(i\ j)$ とすると，

$$\begin{aligned}&\sigma\big(\Delta(x_1,x_2,\cdots,x_n)\big)\\&=(x_1-x_2)\cdots(x_1-x_j)(x_1-x_{i+1})\cdots(x_1-x_i)\cdots(x_1-x_n)\\&\times(x_2-x_3)\cdots(x_2-x_j)(x_2-x_{i+1})\cdots(x_2-x_i)\cdots(x_2-x_n)\\&\quad\times\cdots\cdots\\&\qquad\times(x_{i-1}-x_j)(x_{i-1}-x_{i+1})\cdots(x_{i-1}-x_i)\cdots(x_{i-1}-x_n)\\&\qquad\quad\times\boxed{(x_j-x_{i+1})\cdots(x_j-x_i)}\cdots(x_j-x_n)\\&\qquad\qquad\times\cdots\cdots\quad\boxed{\cdots\cdots}\\&\qquad\qquad\qquad\times\boxed{(x_{j-1}-x_i)}\cdots(x_{j-1}-x_n)\\&\qquad\qquad\qquad\quad\times\cdots\cdots\\&\qquad\qquad\qquad\qquad\times(x_{n-1}-x_n)\\&=(-1)^{2(j-i)-1}\Delta(x_1,x_2,\cdots,x_n)=-\Delta(x_1,x_2,\cdots,x_n).\end{aligned}$$

したがって，任意の置換 σ を互換の合成として，

$$\sigma=\tau_k\,\tau_{k-1}\cdots\tau_1=\sigma_l\,\sigma_{l-1}\cdots\sigma_1\ (\tau_i,\sigma_j：\text{互換})$$

として表すと，

$$\begin{aligned}\sigma\big(\Delta(x_1,x_2,\cdots,x_n)\big)&=(-1)^k\cdot\Delta(x_1,x_2,\cdots,x_n)\\&=(-1)^l\cdot\Delta(x_1,x_2,\cdots,x_n)\end{aligned}$$

よって，$k,\ l$ の偶奇は一致する。

また，奇置換の全体を T_n，$\sigma\in S_n$ を１つの互換とすると，$A_n'=\{\sigma\circ\tau\,|\,\tau\in A_n\}\subset T_n$ で，$\tau\neq\tau'$ のとき $\sigma\circ\tau\neq\sigma\circ\tau'$ であるから，

$$n(A_n)=n(A_n')\leqq n(T_n)$$

同様に，$n(T_n)\leqq n(A_n)$ が示されるから，

$$n(A_n)=n(T_n)=\frac{n!}{2}\qquad\text{（証明終）}$$

次に，対称式の定義を与えよう。

定義：n 変数の多項式 $f(x_1,x_2,\cdots,x_n)$ が，任意の置換 $\sigma\in S_n$ に対して，

$$\begin{aligned}\sigma\big(f(x_1,x_2,\cdots,x_n)\big)&=f(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)})\\&=f(x_1,x_2,\cdots,x_n)\end{aligned}$$

をみたすとき，$f(x_1,\ x_2,\ \cdots,\ x_n)$ は $x_1,x_2,\cdots,x_n$ の対称式であるという。$f(x_1,\ x_2,\ \cdots,\ x_n)$ が $x_1,x_2,\cdots,x_n$ の有理式である場合も，同様に定義する。

（例６）　$s_1=x_1+x_2+\cdots+x_n$，

$$s_2=\sum_{i<j}x_i\,x_j,$$

$$s_3=\sum_{i<j<k}x_i\,x_j\,x_k,$$

$$\cdots,$$

$$s_n=x_1\,x_2\cdots x_n$$

は $x_1,\ x_2,\ \cdots,\ x_n$ の対称式で，基本対称式と呼ばれる。

定理４　任意の対称多項式 $f(x_1,\ x_2,\ \cdots,\ x_n)$ に対し，ある多項式 $g(x_1,\ x_2,\ \cdots,\ x_n)$ で，

$$f(x_1,x_2,\cdots,x_n)=g(s_1,s_2,\cdots,s_n)$$

をみたすものが存在する。

∵ $x_1,x_2,\cdots,x_n$ の単項式 $M=x_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$ に対し，整数の組 $\left(\sum_{i=1}^{n}r_i,r_1,r_2,\cdots,r_n\right)\in{\mathbb{N}_0}^{n+1}$ を対応させ，これを $d(M)$ と表す。また，$\{d(M)\}$ の要素の大小を，$d(M)=(r_0,r_1,\cdots,r_n)$，$d(M')=(r_0',r_1',\cdots,r_n')$ として，

$$d(M)<d(M')\Leftrightarrow r_0=r_0',\cdots,r_{i-1}=r_{i-1}',r_i<r_i'$$

をみたす i が存在する。

ことと定める。（$d(M)$ を M の位数とよぶ。）

対称式 f が単項式 $ax_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$ を含めば，任意の置換 $\sigma\in S_n$ を施して得られる単項式 $a\,x_{\sigma(1)}^{r_1}\,x_{\sigma(2)}^{r_2}\cdots x_{\sigma(n)}^{r_n}$ を含むから，$\sum_{\sigma\in S_n}a\,x_{\sigma(1)}^{r_1}\,x_{\sigma(2)}^{r_2}\cdots x_{\sigma(n)}^{r_n}$ を含み，したがって，$r_1\geqq r_2\geqq\cdots\geqq r_n$ をみたす単項式を含むことを注意しておく。

対称式 f を $f=\sum_i a_iM_i$（M_i：単項式）と表し，f に含まれる単項式の最高位数 $d(M)$ に関する帰納法で証明する。

$d(M)=(0,0,\cdots,0)$ なら，f は定数だから，$f=g$ でよい。

また，$d(M)=(1,\cdots\cdots)$ のときも上の注意より，

$$f=\sum_i a\,x_i=as_1$$

とかけるからよい。

そこで，$M=x_1^{r_1}\,x_2^{r_2}\cdots x_n^{r_n}(r_1\geqq r_2\geqq\cdots\geqq r_n)$ とし，$d(M)$ が $\left(\sum_{i=1}^{n}r_i,r_2,\cdots,r_n\right)$ より小さい対称多項式については，定理の主張が成り立つものとする。

そこで，$g_1(x_1,x_2,\cdots,x_n)=s_n^{r_n}\,s_{n-1}^{r_{n-1}-r_n}\cdots s_2^{r_2-r_3}\,s_1^{r_1-r_2}$ とおけば，g_1 の次数は

$$n r_n + (n-1)(r_{n-1} - r_n) + \cdots + 2(r_2 - r_3) + (r_1 - r_2)$$
$$= r_n + r_{n-1} + \cdots + r_1 = \sum_{i=1}^{n} r_i$$

であり，最高位の単項式は，

$$x_1^{r_n + (r_{n-1} - r_n) + \cdots + (r_1 - r_2)} x_2^{r_n + (r_{n-1} - r_n) + \cdots + (r_2 - r_3)} \cdots x_n^{r_n}$$
$$= x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n}$$

となる。そこで，うまく a をとり，$f - a g_1$ を作れば，これは M より低位数の単項式しか含まない対称式であり，帰納法の仮定から，

$$f - a g_1 = g_2(s_1, s_2, \cdots, s_n)$$

をみたす多項式 $g_2(x_1, x_2, \cdots, x_n)$ がとれる。

よって，

$$g(x_1, x_2, \cdots, x_n) = a x_1^{r_1 - r_2} x_2^{r_2 - r_3} \cdots x_n^{r_n} + g_2(x_1, x_2, \cdots, x_n)$$

とおけば，

$$f(x_1, x_2, \cdots, x_n) = g(s_1, s_2, \cdots, s_n)$$ （証明終）

（例 7）x, y, z の対称式

$$f(x, y, z) = (x-y)^2 + (y-z)^2 + (z-x)^2$$
$$= 2(x^2 + y^2 + z^2) - 2(xy + yz + zx)$$
$$= 2(s_1^2 - 2s_2) - 2s_2 = 2s_1^2 - 6s_2$$

定義：多項式 $f(x_1, x_2, \cdots, x_n)$ が対称式でなく，任意の置換 $\sigma \in S_n$ に対して，$\sigma(f) = \pm f$ をみたすとき，$f(x_1, x_2, \cdots, x_n)$ は $x_1, x_2, \cdots, x_n$ の交代式であるという。

（例 8）差積 $\Delta(x_1, x_2, \cdots, x_n) = \prod_{i<j}(x_i - x_j)$ は，偶置換 σ に対して，$\sigma(\Delta(x)) = \Delta(x)$，奇置換 τ に対して，$\tau(\Delta(x)) = -\Delta(x)$ をみたすから，交代式である。

実は，次の定理が成り立つ。

定理 5　任意の交代式 $f(x_1, x_2, \cdots, x_n)$ は，差積 $\Delta(x_1, x_2, \cdots, x_n)$ と対称式の積で表される。

㊀置換 $\sigma \in S_n$ に対して，$\sigma(f) = \varepsilon(\sigma) \cdot f \ (\varepsilon(\sigma) = \pm 1)$ により $\varepsilon(\sigma)$ を定義する。$\tau \in S_n$ とすれば，

$$(\tau \circ \sigma)(f) = \tau(\sigma(f)) = \tau(\varepsilon(\sigma) \cdot f) = \varepsilon(\sigma) \cdot \varepsilon(\tau)(f)$$

であるから，$\varepsilon(\tau \circ \sigma) = \varepsilon(\tau)\varepsilon(\sigma)$ が成り立つ。

また，任意の置換は互換の合成で表されるから，ある互換 $\tau = (i\ j)$ に対して，$\varepsilon(\tau) = -1$ となる。

すなわち，

$$f(x_1, \cdots, x_j, \cdots, x_i, \cdots, x_n) = -f(x_1, \cdots, x_i, \cdots, x_j, \cdots, x_n)$$

よって，$f(x_1, \cdots, x_i, \cdots, x_i, \cdots, x_n) = 0$ であり，$f(x_1, x_2, \cdots, x_n)$ は $x_i - x_j$ で割り切れる。今，$f(x_1, x_2, \cdots, x_n)$ が $(x_i - x_j)^h$ で割り切れ，$(x_i - x_j)^{h+1}$ で割り切れないとすると，$f^2(x_1, x_2, \cdots, x_n)$ は $(x_i - x_j)^{2h}$ で割り切れる。f^2 は対称式であるから，$(\Delta(x))^{2h}$ で割り切れることになり，

$$f(x_1, x_2, \cdots, x_n) = (\Delta(x))^h \cdot f_1(x_1, x_2, \cdots, x_n)$$

とかける。$f_1(x_1, x_2, \cdots, x_n) = \dfrac{f}{(\Delta(x))^h}$ であるから，任意の $\sigma \in S_n$ に対して，

$$\sigma(f_1) = \pm f_1$$

が成り立つ。ある互換 $\rho = (k\ l)$ に対して，$\rho(f_1) = -f_1$ が成り立てば，上と同様にして，f_1 が差積 $\Delta(x)$ で割り切れることになり，h の最大性に反する。

したがって，任意の互換 σ に対して $\sigma(f_1) = f_1$ が成り立たねばならず，f_1 は対称式である。

$f(x_1, x_2, \cdots, x_n)$ は交代式だから，h は奇数であり，$h = 2h_1 + 1 \ (h_1 \geqq 0)$ とかける。よって，

$$g(x_1, x_2, \cdots, x_n) = (\Delta(x))^{2h_1} \cdot f_1(x_1, x_2, \cdots, x_n)$$

とおけば，$g(x_1, x_2, \cdots, x_n)$ は $x_1, x_2, \cdots, x_n$ の対称式であり，

$$f(x_1, x_2, \cdots, x_n) = \Delta(x) \cdot g(x_1, x_2, \cdots, x_n)$$

とかける。 （証明終）

この証明から，A_n, T_n を偶置換の全体，奇置換の全体とすれば，交代式 f について

$\sigma \in A_n$ のとき，$\sigma(f) = f$

$\tau \in T_n$ のとき，$\tau(f) = -f$

が成り立つことが分かる。

（参考）$\sigma, \tau \in S_n$ のとき，$\tau \circ \sigma \in S_n$ であり，

1）$\rho \circ (\tau \circ \sigma) = (\rho \circ \tau) \circ \sigma \quad (\sigma, \tau, \rho \in S_n)$

2）$1_n \circ \sigma = \sigma \circ 1_n = \sigma \quad (\sigma \in S_n)$

3）$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1_n \ (\sigma \in S_n)$

が成り立つことを，S_n は群をなすという。また，A_n は S_n の合成で閉じており，1），2），3）をみたす。

このことを，A_n は S_n の部分群をなすという。

これに関連して，次の定理が成り立つ。

定理 6　n 変数の多項式 $f(x_1, x_2, \cdots, x_n)$ に変数の置換を施して得られる多項式の全体が

$$f = f_1, f_2, \cdots, f_l$$

であるとき，

1）l は $n!$ の約数である。

2）$H_1 = \{\sigma \in S_n \mid \sigma(f) = f\}$ は，S_n の部分群をなす。

㊀2）H_1 は S_n の部分群をなす。

∵）$\tau, \sigma \in H_1$ とすると，$(\tau \circ \sigma)(f) = \tau(\sigma(f)) = \tau(f) = f$ よって，$\tau \circ \sigma \in H_1$

また，明らかに，$1_n \in H_1$ であり，$\sigma \in H_1$ のとき，

$$\sigma^{-1}(f) = \sigma^{-1}(\sigma(f)) = (\sigma^{-1} \circ \sigma)(f) = 1_n(f) = f$$

が成り立つから，$\sigma^{-1} \in H_1$

以上より，H_1 は S_n の部分群をなす。

1）$H_i = \{\sigma \in S_n \mid \sigma(f) = f_i\}$ とおくと，$i \neq j$ のとき，$H_i \cap H_j = \phi$ で，$n(H_i) = n(H_j)$ さらに，$n! = l \cdot n(H_1)$ が成り立つ。

∵）$\sigma \in H_i \cap H_j (i \neq j)$ とすれば，$\sigma(f) = f_i, \sigma(f) = f_j$ であるから，$f_i = f_j$ これは，$f_i \neq f_j$ に反する。

$\therefore H_i \cap H_j = \phi$

$n(H_i)=n(H_j)$を示すには，$n(H_1)=n(H_i)$をいえばよい。

$H_1=\{\sigma_1,\sigma_2,\cdots,\sigma_r\}$とし，$\sigma\in H_i$とすれば，$\sigma\circ\sigma_1$，$\sigma\circ\sigma_2$，$\cdots$，$\sigma\circ\sigma_r$はすべて異なり，

$$\{\sigma\circ\sigma_1,\sigma\circ\sigma_2,\cdots,\sigma\circ\sigma_r\}\subset H_i$$

よって，$n(H_1)\leqq n(H_i)$

逆に，$H_i=\{\tau_1,\tau_2,\cdots,\tau_s\}$とすれば，$1,\ \tau_1^{-1}\circ\tau_2,\ \cdots,\ \tau_1^{-1}\circ\tau_s$はすべて異なり，

$$\{1,\tau_1^{-1}\circ\tau_2,\cdots,\tau_1^{-1}\circ\tau_s\}\subset H_1$$

よって，$n(H_i)\leqq n(H_1)\quad\therefore n(H_1)=n(H_i)$

これより，

$$\begin{aligned}n!=n(S_n)&=n(H_1\cup H_2\cup\cdots\cup H_l)\\&=n(H_1)+n(H_2)+\cdots+n(H_l)\\&=l\cdot n(H_1)\end{aligned}$$

（証明終）

また，次の定理が成り立つ。

定理7　n 変数の有理式 $f(x_1,\ x_2,\ \cdots,\ x_n)$から文字の置換によって得られる有理式を

$$f=f_1,\ f_2,\ \cdots,\ f_l$$

とするとき，$f_1,\ f_2,\ \cdots,\ f_l$ についての対称式 $\varphi(f_1,\ f_2,\ \cdots,f_l)$ は，$x_1,\ x_2,\ \cdots,\ x_n$の対称式である。

∵$\sigma\in S_n$のとき，$\sigma(f_i)\neq\sigma(f_j)\ (i\neq j)$であるから，$\sigma(f_1),\ \sigma(f_2),\ \cdots,\ \sigma(f_l)$ の全体は，$f_1,\ f_2,\ \cdots,\ f_l$ の全体と一致する。したがって，$f_1,\ f_2,\ \cdots,\ f_l$ の対称式 $\varphi(f_1,\ f_2,\ \cdots,f_l)$について，

$$\begin{aligned}\sigma\big(\varphi(f_1,f_2,\cdots,f_l)\big)&=\varphi\big(\sigma(f_1),\sigma(f_2),\cdots,\sigma(f_l)\big)\\&=\varphi(f_1,f_2,\cdots,f_l)\end{aligned}$$

が成り立つ。したがって，$\varphi(f_1,\ f_2,\ \cdots,f_l)$は$x_1,x_2,\cdots,x_n$の対称式である。

4. 体の巾根拡大

整数の全体$\mathbb{Z}$や実数係数多項式の全体 $\mathbb{R}[x]$ では，加減乗の計算が自由にでき，交換法則，結合法則，分配法則が成り立つ。このような数あるいは式の集合を（可換）環という。

また，有理数の全体 $\mathbb{Q}$ や実数の全体 $\mathbb{R}$ は環である上に，0でない数による除法ができる。このような環を体という。

以上の用語を準備した上で，まず次の補題を証明しよう。

補題1　$\mathbb{Z}$を整数環とし，2つの整数 $p,\ q$ が互いに素であるとすると，

$$ph+ql=1$$

をみたす整数 h,l が存在する。

∵集合 $I=\{ph+ql\,|\,h,l\in\mathbb{Z}\}\subset\mathbb{Z}$ を考える。$x\in I$とすれば，$x=ph+ql\ (h,l\in\mathbb{Z})$とかけるから，$-x=p\cdot(-h)+q\cdot(-l)\in I$ また，$p,\ q\in I(p\neq0,\ q\neq0)$であるから，$I$は正の整数を含む。そこで，$I$に含まれる正の整数で最小のものを$x_0=ph_0+ql_0$とし，$I$の任意の要素 x を x_0 で割ったときの商を s，余りを r $(0\leqq r<x_0)$ とすると，$x=x_0\,s+r$より，

$$\begin{aligned}r&=x-x_0s=(ph+ql)-(ph_0+ql_0)\cdot s\\&=p(h-h_0\,s)+q\cdot(l-l_0\,s)\in I\end{aligned}$$

x_0 の最小性より，$r=0$ すなわち，Iのすべての要素 x は x_0 の倍数。$p,\ q\in I$であるから，x_0 は p,q の公約数であるが，仮定より，p,q は互いに素だから，$x_0=1$

$$\therefore\ p\,h_0+q\,l_0=1$$

（証明終）

全く同様にして，次の補題2を証明することができる。ただし，x_0 に相当するものは，Iに属する最低次数の整式である。

補題2　Kを体，$K[x]$ を Kに係数をもつ1変数多項式環とする。2つの多項式$f(x)$，$g(x)$が互いに素であれば，

$$f(x)h(x)+g(x)\,l(x)=1$$

をみたす多項式 $h(x),\ l(x)\big(\in K[x]\big)$が存在する。

（$f(x),\ g(x)$ を同時に割り切る多項式が定数のみであるとき，$f(x)$ と $g(x)$ は互いに素であるという。）

方程式 $f(x)=0$ が体 K の中に根をもたなくても，K を含む体 K' で根をもつことはあり得る。——（代数学の基本定理）そのような場合についての一結果を証明しよう。

定理8　Kを体，pを素数，$r\in K_{s.t.}\ \sqrt[p]{r}\notin K$とする。このとき，$K$の要素と$\sqrt[p]{r}$から四則によって得られる数の全体を$K\big(\sqrt[p]{r}\big)$とすれば，その要素は，$K$の要素$a_0,\ a_1,\ a_2,\ \cdots,\ a_{p-1}$を用いて，

$$a_0+a_1\sqrt[p]{r}+a_2\big(\sqrt[p]{r}\big)^2+\cdots+a_{p-1}\big(\sqrt[p]{r}\big)^{p-1}\quad\text{——(1)}$$

の形にただ一通りに表すことができる。

∵Kの要素を $a,b,c,\cdots$ で表し，$\alpha=\sqrt[p]{r}$とおく。

また，$\varepsilon=\cos\dfrac{2\pi}{p}+i\sin\dfrac{2\pi}{p}$（1の$p$乗根）とおく。

1）$K(\alpha)$ の要素は(1)の形に表される。

∵）Kの要素と α の加減乗で得られる要素は，

$$a_0+a_1\alpha+a_2\alpha^2+\cdots+ap\alpha^p+\cdots$$

とかけるが，$\alpha^p=r\in K$であるから，$\alpha^n(n\geqq p)$の形の項はこの関係を用いて，$1,\ \alpha,\ \cdots,\ \alpha^{p-1}$ で表すことができる。従って，$K(\alpha)$ の要素は，

$$\xi=\frac{b_0+b_1\alpha+\cdots+b_{p-1}\,\alpha^{p-1}}{c_0+c_1\alpha+\cdots+c_{p-1}\alpha^{p-1}}\quad\text{——(2)}$$

とかける。この右辺の分子を$f(\alpha)$，分母を$g(\alpha)$として，

$$\xi=\frac{f(\alpha)\,g(\varepsilon\alpha)\cdots g(\varepsilon^{p-1}\alpha)}{g(\alpha)\,g(\varepsilon\alpha)\cdots g(\varepsilon^{p-1}\alpha)}$$

と変形すると，分母は$x^p-r=0$の根 $\alpha,\ \varepsilon\alpha,\cdots,\ \varepsilon^{p-1}\alpha$ に関する対称式であるから，$c_0,\ c_1,\ \cdots,\ c_{p-1}$

r（r 以外の基本対称式の値は 0）の整式に等しく，K の要素（これを d とする）である。

また，分子で，$g(\varepsilon\alpha)\cdots g(\varepsilon^{p-1}\alpha)$ は方程式

$$x^{p-1}+\alpha x^{p-2}+\alpha^2x^{p-3}+\cdots+\alpha^{p-2}x+\alpha^{p-1}=0$$

の根 $\varepsilon\alpha,\ \varepsilon^2\alpha,\ \cdots,\ \varepsilon^{p-1}\alpha$ の対称式であるから，$c_0,\ c_1,\ \cdots,\ c_{p-1}$ および α（根の基本対称式の値は $\pm\alpha^k$ の形）の整式に等しく，したがってそれに $f(\alpha)$ をかけて得られる ξ の分子は，K に係数をもつ α の整式として，

$$k_0+k_1\alpha+\cdots+k_{p-1}\alpha^{p-1}$$

とかける。よって，

$$\xi=\frac{1}{d}(k_0+k_1\alpha+\cdots+k_{p-1}\alpha^{p-1})$$

と表され，(1)の形となる。

(2) $K(\alpha)$ の要素の(1)の形の表し方は，一意的である。

∵）仮に，ξ の(1)の形での表し方が2通りあるとすれば，その差をとって，

$$F(\alpha)=r_0+r_1\alpha+\cdots+r_{p-1}\alpha^{p-1}=0 \qquad \text{——(3)}$$

とかける。

まず，x^p-r が既約多項式であることを示そう。

$$x^p-r=(x^m+\cdots\pm c)(x^{p-m}+\cdots+d)\quad(0<m<p)$$

とすれば，$x^p-r=\prod_{i=1}^{p}(x-\varepsilon^i\alpha)$ であるから，c は $\alpha,\ \varepsilon\alpha,\ \cdots,\ \varepsilon^{p-1}\alpha$ の中の m 個の積に等しい。

$\therefore\ \varepsilon'\alpha^m=c$　（ε' はいくつかの ε の積）

$$c^p=(\varepsilon'\alpha^m)^p=(\varepsilon')^p\cdot(\alpha^p)^m=1\cdot r^m=r^m$$

$0<m<p$ で，p は素数であるから，p と m は互いに素で，

$$mh=pk+1$$

をみたす整数 h, k が存在する。これより，

$$c^{ph}=r^{mh}=r^{pk+1}=r^{pk}\cdot r\quad\therefore\ r=\left(\frac{c^h}{r^k}\right)^p$$

これは，$\alpha=\sqrt[p]{r}\notin K$ に矛盾する。よって，x^p-r は既約多項式でなければならない。

次に，α を根にもつ方程式 $f(x)=0$ で，$f(x)$ の次数が最低のものを $f_0(x)=0$ とする。x^p-r を $f_0(x)$ で割ったときの商を $q_0(x)$，余りを $r_0(x)$ $\left(\deg r_0(x)<\deg f_0(x)\right)$ とすれば，

$$x^p-r=f_0(x)q_0(x)+r_0(x)$$

x に α を代入して，

$$0=\alpha^p-r=f_0(\alpha)q_0(\alpha)+r_0(\alpha)$$

$\therefore\ r_0(\alpha)=0$

$f_0(x)$ の次数の最小性から，$r_0(x)=0$

$\therefore\ x^p-r=f_0(x)\,q_0(x)$

上に示したように，x^p-r は既約であり，$f_0(x)$ の次数は2以上であるから，$q_0(x)$ は定数である。よって，$f_0(x)=x^p-r$ と考えてよい。

上の議論から，$F(x)$ は $f_0(x)=x^p-r$ で割り切れなければならないが，$\deg F(x)<\deg f_0(x)=p$ であるから，$F(x)=0$

$\therefore\ r_0=r_1=\cdots=r_{p-1}=0$

すなわち，ξ の(1)の形の表し方はただ一通りである。

5. 主定理の証明

まずは，方程式が代数的に解ける，あるいは巾根（累乗根のこと）を用いて解けることの意味を考えてみる。

有理数係数の2次方程式 $x^2-2x-1=0$ は有理数体 $\mathbb{Q}$ 内で解くことはできないが，$\mathbb{Q}$ に $\sqrt{2}$ を付け加えた体 $\mathbb{Q}(\sqrt{2})$ においては解けて，その根は，$x=1\pm\sqrt{2}$ である。

また，3次方程式 $x^3+3x-1=0$ を解くには，$x=y-\dfrac{1}{y}$ とおいて，

$$\left(y-\frac{1}{y}\right)^3+3\left(y-\frac{1}{y}\right)-1=0$$

$$y^3-1-\frac{1}{y^3}=0,\ \text{すなわち},\ (y^3)^2-y^3-1=0$$

これより，$y^3=\dfrac{1\pm\sqrt{5}}{2}$ よって，求める根は，

$$x=\sqrt[3]{\frac{1+\sqrt{5}}{2}}+\sqrt[3]{\frac{1-\sqrt{5}}{2}},\ \omega\sqrt[3]{\frac{1+\sqrt{5}}{2}}+\omega^2\sqrt[3]{\frac{1-\sqrt{5}}{2}},$$

$$\omega^2\sqrt[3]{\frac{1+\sqrt{5}}{2}}+\omega\sqrt[3]{\frac{1-\sqrt{5}}{2}}\qquad(\omega\text{ は1の立方根})$$

したがって，この3次方程式を解くには，まず $\mathbb{Q}$ に $\sqrt{5}$ を付け加えた $\mathbb{Q}(\sqrt{5})$，続いてそれに $\sqrt[3]{\dfrac{1+\sqrt{5}}{2}}$ や ω などを付け加えた体 $\mathbb{Q}(\sqrt{5},\ \omega,\ \cdots)$ を考えればよいことが分かる。こうして，次の定義に到る。

定義：体 K に係数をもつ n 次方程式 $x^n+a_1x^{n-1}+\cdots+a_n=0$ が K に巾根を有限回加えた体 K' で根をもつならば，この n 次方程式は代数的に解けるあるいは巾根によって解けるという。

こうして，本定理の証明に必要な次の補題を述べることができる。

補題3　n 次方程式 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n=0$ が巾根のみによって解けるならば，解法に必要な素数次の巾根 $\sqrt[p]{r}$，$\sqrt[q]{r_1}$，…は，$f(x)=0$ の根 $x_1, x_2, \cdots x_n$ と1の p 乗根，1の q 乗根，…の有理式として表すことができる。（$\sqrt[6]{r}$ が必要なときは，$\sqrt[3]{r}=r_1$，$\sqrt{r_1}$ の2つの素数次の巾根に分けられるから，素数次の巾根のみでよい。）

㊟1）方程式 $f(x)=0$ の解法に必要な巾根で，最後

に追加するものを $\alpha=\sqrt[p]{r}$（$r\in K$, $\alpha\notin K$ ただし，K 自身，そのような巾根を追加しながら拡張された体である）として，$f(x)=0$ の1つの根 x_1 が，

$$x_1=r_0+r_1\alpha+\cdots+r_{p-1}\alpha^{p-1}\quad(r_i\in K)\qquad\text{——(1)}$$

と表されるとき，$r_1=1$ としてよい。

∵）$r_1\neq 0$ であれば

$$x_1=r_0+r_1\alpha+\frac{r_2}{r_1^{\,2}}(r,\alpha)^2+\cdots+\frac{r_{p-1}}{(r_1)^{p-1}}(r_1\alpha)^{p-1}$$

だから，α を $r_1\alpha$ に取りかえても，$r_1\alpha\notin K, (r_1\alpha)^p=r_1{}^p r\in K$ かつ $K(\alpha)=K(r_1\alpha)$ で差し支えない。次に，r_0 以外のすべての r_i が0とすると，$x_1\in K$ であり，α は不要である。そこで，(1)の右辺の r_i で $r_i\neq 0\,(i>0)$ となる最初のものを $r_m\,(0<m<p)$ とする。p は素数だから，$mh-pk=1$ をみたす整数 h, k をとれば，

$$\alpha=\alpha^{mh-pk}=\frac{\alpha^{mh}}{\alpha^{pk}}=\frac{(\alpha^m)^h}{r^k}$$

よって，$\alpha'=r_m\alpha^m$ とおくと，

$$\alpha=\frac{(r_m\alpha^m)^h}{r_m{}^h r^k}=\frac{(\alpha')^h}{r_m{}^h r^k}$$

であり，α の累乗は α' の累乗に K に属する数をかけて得られる。また，$(\alpha')^p=r_m{}^p r^m\in K$ であるから，α' の累乗は1，α', …, $(\alpha')^{p-1}$ に K に属する数をかけたものの和として表される。

しかも，$m<m'<p$ のとき，$m'h=pl'+1$ をみたす整数 l' があったとすると，

$$\alpha^{m'}=\left(\frac{1}{r_m{}^h\cdot r^k}\right)^{m'}\cdot(\alpha')^{m'h}=\frac{r_m{}^{pl'}\cdot r^{ml'}}{(r_m{}^h\cdot r^k)^{m'}}\cdot\alpha'$$

とかけるはずであるが，

$$h(m-m')=(pk+1)-(pl'+1)=p(k-l')$$

より，$h(m-m')$ が p で割り切れることになるからありえない。よって，(1)は

$$x_1=r_0'+\alpha'+r_2'(\alpha')^2+\cdots+r_{p-1}'(\alpha')^{p-1}\quad(r_i'\in K)$$

の形に表される。α を α' に取りかえてもよいから，

$$x_1=r_0+\alpha+r_2\alpha^2+\cdots+r_{p-1}\alpha^{p-1}\qquad\text{——(1)}$$

の形にかけることが示された。

2）次に，$f(x)=0$ が巾根によって解けるなら，解法に必要となる最後の巾根 $\alpha=\sqrt[p]{r}$ は，$x_1, x_2, \cdots, x_n$ と1の p 乗根 ω の有理式として表されることを示す。

∵）まず，$f(x)$ に $x=x_1=r_0+\alpha+r_2\alpha^2+\cdots+r_{p-1}\alpha^{p-1}$ を代入して整理すると，$\alpha^p=r\in K$ より，

$$f(x_1)=s_0+s_1\alpha+\cdots+s_{p-1}\alpha^{p-1}\quad(s_i\in K)$$

となるが，$f(x_1)=0$ であるから前補題の一意性により，

$$s_0=s_1=\cdots=s_{p-1}=0\qquad\text{——(2)}$$

今，x_1 の代わりに，

$$r_0+\omega\alpha+r_2(\omega\alpha)^2+\cdots+r_{p-1}(\omega\alpha)^{p-1}$$

を $f(x)$ に代入すると，

$$s_0+s_1(\omega\alpha)+\cdots+s_{p-1}(\omega\alpha)^{p-1}$$

を得るが，(2)により，この値は0に等しい。以下，同様に考えて，$1\leqq i\leqq p$ のとき，

$$x_i=r_0+\omega^{i-1}\alpha+r_2(\omega^{i-1}\alpha)^2+\cdots+r_{p-1}(\omega^{i-1}\alpha)^{p-1}$$

がすべて $f(x)=0$ の根であることが分かる。

これらの式に，1, 1, …, 1 あるいは，1, ω^{-1}, …, $\omega^{-(p-1)}$，あるいは，1, ω^{-2}, ω^{-4}, …, $\omega^{-2(p-1)}$, … をかけて辺々加えると，次の諸式を得る。

$$\left.\begin{aligned}
r_0&=\frac{1}{p}(x_1+x_2+\cdots+x_p)\\
\alpha&=\frac{1}{p}\left(x_1+\omega^{-1}x_2+\cdots+\omega^{-(p-1)}x_p\right)\\
r_2\alpha^2&=\frac{1}{p}\left(x_1+\omega^{-2}x_2+\cdots+\omega^{-2(p-1)}x_p\right)\\
&\cdots\cdots\cdots\cdots\\
r_{p-1}\alpha^{p-1}&=\frac{1}{p}\left(x_1+\omega^{-(p-1)}x_2+\cdots+\omega^{-(p-1)^2}x_p\right)
\end{aligned}\right\}\text{-(3)}$$

これらから，α, r_0, r_2, …, r_{p-1} が $f(x_1)=0$ の根 $x_1, x_2, \cdots, x_p$ と1の p 乗根 ω の有理式として表されることが分かる。

3）最後に，α より前に必要となる巾根が，$f(x)=0$ の根 $x_1, x_2, \cdots, x_n$ と1の累乗根の有理式として表されることを示す。

∵）(1)において，r_0, r_2, …, r_{p-1} は巾根による解法で必要となる巾根の最後のもの以外を付加してできる体 K に属するから，最後より前の巾根しか含まない。r_0, r_2, …, r_{p-1} のうちの1つを y_0 とすると，$f(x)=0$ の根 $x_1, x_2, \cdots, x_p$ と1の p 乗根を含む有理式 φ があって，

$$y_0=\varphi(x_1, x_2, \cdots, x_p)$$

とかける。いま，y_0 の式から $x_1, x_2, \cdots, x_n$ の置換によって得られる値のすべてを y_0, y_0', …, $y_0^{(s)}$ とし，

$$\begin{aligned}F(y)&=(y-y_0)(y-y_0')\cdots(y-y_0{}^{(s)})\\&=y^s-t_1y^{s-1}+t_2y^{s-2}+\cdots+(-1)^s t_s\end{aligned}$$

とおくと，$t_1, t_2, \cdots, t_s$ は y_0, y_0', …, $y_0^{(s)}$ の基本対称式である。$x_1, x_2, \cdots, x_n$ の任意の置換により集合 $\{y_0, y_0', \cdots, y_0^{(s)}\}$ は不変であり，したがって $F(y)$ も不変であるから，$t_1, t_2, \cdots, t_s$ は $x_1, x_2, \cdots, x_n$ の対称式となる。したがって，y_0 は $f(x)=0$ の係数（$x_1, x_2, \cdots, x_n$ の基本対称式に±1をかけたもの）と1の p 乗根 ω から有理的に導かれた数を係数にもつ方程式 $F(y)=0$ の根である。

y_0 は，$f(x)=0$ の解法で，最後より前に出てくる巾根と1の累乗根を含む式であるから，含まれている巾根の中で最後のもの β は（β は方程式 $F(y)$

$=0$ を解くために必要な最後の巾根となるから，

2）における α の同じく） y_0, y_0', $\cdots$, $y_0^{(s)}$ と1の累乗根によって有理的に表される。y_0, y_0', $\cdots$, $y_0^{(s)}$ 自身は $x_1, x_2, \cdots, x_n$ の有理式であるから，この巾根 β も $f(x)=0$ の根 $x_1, x_2, \cdots, x_n$ と1の累乗根の有理式で表される。$f(x)=0$ の解法で必要となる巾根は有限個であるから，この論法を有限回行うことにより，必要な巾根のすべてが $f(x)=0$ の根と1の累乗根の有理式として表されることが分かる。

以上の準備のもとに，目標の本定理を証明することができる。

定理9　（アーベル）5次以上の方程式

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_n=0$$

は，一般に，これを巾根によって解くことはできない。

㋐方程式 $f(x)=0$ が巾根によって解けると仮定して矛盾を導く。

1）方程式 $f(x)=0$ を解くために，基礎の体 K に最初に付け加えるべき巾根を $\sqrt[p]{r}$（p：素数，$r\in K$, $\sqrt[p]{r}\notin K$）とすれば，$p=2$ で，$K_1=K\left(\sqrt{r}\right)$ の要素を不変にする置換 $\sigma\in S_n$ の全体を H とすると，

$H=A_n$

∵）基礎の体 K は係数 a_1, a_2, …, a_n の有理式全体から成るから，$x_1, x_2, \cdots, x_n$ の有理対称式の全体に等しい。この体 K に付け加えるべき最初の巾根を $\sqrt[p]{r}$（p：素数，$r\notin K$, $\sqrt[p]{r}\notin K$）とすれば，補題3により，それは1の累乗根と $f(x)=0$ の根 $x_1, x_2, \cdots, x_n$ の有理式として，

$$\sqrt[p]{r}=\varphi(x_1, x_2, \cdots, x_n)$$

のように表せる。しかし，K の要素ではないから φ は対称式ではなく，$\varphi^p=r\in K$ より，φ^p が a_1, a_2, …, a_n の有理式。したがって，$x_1, x_2, \cdots, x_n$ の対称式となる。

φ は対称式でないから，ある互換，たとえば $\sigma=(1\,2)$ によって，別の式 φ' に変わる。

$$\sigma(\varphi)=\varphi'\ (\neq\varphi) \qquad \text{——(1)}$$

一方，φ^p は対称式であるから，

$$(\varphi')^p=\sigma(\varphi^p)=\varphi^p$$

$$\therefore\ \varphi'=\varepsilon\varphi \quad (\varepsilon \text{ は1の } p \text{ 乗根}) \qquad \text{——(2)}$$

(2)は $x_1, x_2, \cdots, x_n$ の恒等式で，$\sigma^2=1$ だから，

$\sigma(\varphi')=\varepsilon\sigma(\varphi)=\varepsilon\varphi'$ より $\varphi=\varepsilon\varphi'$

これより，

$$\varphi=\varepsilon\varphi'=\varepsilon(\varepsilon\varphi)=\varepsilon^2\varphi \quad \therefore\ \varepsilon^2=1$$

$\varepsilon\neq1$ より，$\varepsilon=-1$

$\varepsilon^p=1$，かつ p は素数であるから，$p=2$

したがって，最初に付け加えるべき巾根は平方根で，それはある互換によって符号を変える x_1, x_2, …, x_n の交代式でなければならない。従って，

$$\sqrt{r}=\varphi(x_1, x_2, \cdots, x_n)$$
$$=\Delta(x)\cdot S(x_1, x_2, \cdots, x_n) \quad (S\text{：対称式})$$

と表され，$K_1=K\left(\sqrt{r}\right)$ の要素 $k_1+k_2\sqrt{r}$（$k_i\in K$ より，k_i は $x_1, x_2, \cdots, x_n$ の対称式）は

$S_1(x)+\Delta(x)\cdot S_2(x)$（$S_i$：$x_1, x_2, \cdots, x_n$ の対称式）の形である。これらは偶置換の全体 A_n で不変であるから，$K_1=K\left(\sqrt{r}\right)$ の要素を不変にする置換 $\sigma\in S_n$ の全体を H とすれば，$H\supset A_n$

定理6と同様にして，H が S_n の部分群をなし，$n(H)$ が $n(S_n)$ の約数であることが示されるから，

$$n(A_n)\leqq n(H)<n(S_n),\quad n(S_n)=2\times n(A_n)$$

より，$n(H)=n(A_n)$，したがって，

$H=A_n$

2）次に K_1 に付け加えるべき巾根を $\sqrt[q]{r_1}$（q：素数，$r_1\in K_1$, $\sqrt[q]{r_1}\in K_1$）とすると，$q=3$

∵）$\sqrt[q]{r_1}$ が，1の累乗根を $f(x)=0$ の根 $x_1, x_2, \cdots, x_n$ の有理式により，$\sqrt[q]{r_1}=\psi(x_1, x_2, \cdots, x_n)$ と表されるものとする。

上で見たように，1の累乗根と $f(x)=0$ の根 x_1, x_2, …, x_n の有理式全体の中で，K_1 の要素は偶置換の全体 A_n で不変であった。逆に，ある x_1, x_2, …, x_n の有理式 ξ が偶置換の全体で不変であるとすれば，任意の互換 σ_0 について，$S_n=A_n\cup(\sigma_0\cdot A_n)$ が成り立つから，集合

$$\left\{\sigma(\xi)\,\middle|\,\sigma\in S_n\right\}$$

は，高々2つの要素をもつ。

$\sigma_0(\xi)=\xi$ ならば，ξ は S_n で不変であるから，x_1, x_2, …, x_n の対称式であり，K_1 に属する。また，

$\sigma_0(\xi)=\xi'$ $(\xi\neq\xi')$

とすれば，$\varphi_1=\xi+\xi'$ は対称式であり，$\psi_1=\xi-\xi'$ は交代式となる。このとき，

$$\xi=\frac{1}{2}(\varphi_1+\psi_1)$$

とかけるから，$\xi\in K_1$

すなわち，1の累乗根と $f(x)=0$ の根 x_1, x_2, …, x_n の有理式全体の中で，偶置換の全体 A_n で不変なものの全体が K_1 である。

ところで，$\sqrt[q]{r_1}=\psi$ はこの K_1 に属さないから，ある偶置換 τ をとれば，

$\tau(\psi)\neq\psi$

が成り立つ。一方，任意の偶置換は偶数個の互換の合成であり，

$$(1\,a)(1\,b)=(1\,a)(1\,2)(1\,2)(1\,b)$$
$$=(1\,2\,a)(1\,b\,2)$$

が成り立つから，任意の偶置換は長さ3の巡回置換の合成である。したがって，τ として長さ3の

巡回置換，たとえば，$\tau=(123)$ がとれる。そこで，$\tau(\psi)=\psi'(\psi\neq\psi')$とおくと，$\psi^q\in K_1$だから偶置換で不変であり，

$\psi^q=\tau(\psi^q)=\tau(\psi)^q=(\psi')^q$

$\therefore\ \psi'=\omega\psi$　（ωは1のq乗根で，$\omega\neq1$）—(3)

これより，

$\tau^3(\psi)=\tau^2(\psi')=\omega\tau^2(\psi)=\omega^3\psi$

であるが，$\tau^3=1$であるから，

$\psi=\omega^3\psi$　$\therefore\omega^3=1$

$\omega\neq1$で，$\omega^q=1$をみたすから，qは3の倍数であるが，qは素数より，$q=3$

したがって，第2回目に加えるべき巾根は3乗根でなければならない。

3） 5次以上の方程式は，一般に巾根だけで解くことはできない。

∵） $n\geqq5$ の場合，長さ5の巡回置換 $\tau'=(a\,b\,c\,d\,e)$ は$\tau'=(a\,c)(a\,d)(a\,c)(a\,b)$と表せるから偶置換である。したがって，$\psi^3\in K_1$より，

$\tau'(\psi^3)=\psi^3$

$\tau'(\psi^3)=\tau'(\psi)^3$であるから，$\psi$が$\tau'$によって変わるとしても$\tau'(\psi)$は$\psi$に1の立方根$\omega$を乗じたものでしかありえない。

ところが，$(\tau')^5=1$であるから，ψにτ'を5回施せば，

$(\tau')^5(\psi)=(\tau')^4(\omega\psi)=\cdots=\omega^5\psi$

より，$\omega^5=1$

ωは1の立方根であるから，$\omega=1$でなければならず，したがって，ψはτ'で不変である。

ところが，

$(32154)(13245)=(123)$

であるから，ψは$\tau=(123)$で不変である。これは(3)に矛盾する。

したがって，1の累乗根と$x_1,x_2,\cdots,x_n$の有理式ψで，

i） $\sigma(\psi)\neq\psi$をみたす偶置換σが存在する。

ii） 素数$q(\geqq3)$があり，ψ^gは任意の偶置換に対して不変である。

ようなものは存在しない。

このことは，方程式$f(x)=0$が巾根で解けるとすれば，ただ1つの平方根だけで解けることを示しており，$K_1=\left\{k_1+k_2\sqrt{r}\,\middle|\,k_i\in K,r\in K,\sqrt{r}\notin K\right\}$より，

$x_1=S_1(x)+\Delta(x)\cdot S_2(x)$ (S_1,S_2：対称式)

とかける。しかし，右辺は任意の偶置換で不変であり，したがって恒等式ではあり得ない。

すなわち，5次以上の方程式は一般に巾根のみで解くことはできない。　（証明終）

6. 反省と課題

数学史の本を繙くとき，数学的概念の発達に伴う多くの苦悩や感動があることに気付く。方程式論の歴史も，中・高以来の学習と関連して身近で興味深いものであるが，古代バビロニアから中世イタリアを経てガロアによる完全な解決に至る流れは劇的でさえある。

現在の大学では，学部での代数学の講義に関わって群・環・体論を学び，ガロア理論もその中で触れられるのが通常である。その中で展開される体の自己同型群と不変体の対応関係は見事なものであり，ガロアの偉大さを感じとるには十分であるが，こと方程式論に限っていえば，抽象的に整理されすぎていて，方程式論解決に至るまでの先人の思考の流れを辿ることは難しい。

そうした中，偶然にも数学研究班の生徒から“アーベルの理論”，あるいは“ガロアの理論”について講義をして欲しいとの声が上がり，果して高校生に理解させることができるのか，可能だとすればどのような扱いになるのかと自問自答した。

その結果，予備知識が少なく，議論の流れが分かりやすいのはアーベルの論文であろうとの結論に至り，そのものではないが，それに近い扱いの高木貞治著「代数学講義」に倣うことにした。

実際の講義では，高校1年生が3名，高校2年生が5名ほぼ最後まで聞いたが，高校1年生には定理4，5の対称式，交代式に関する内容が精一杯であったと思う。高校2年生は変数の置換群と対称式との関連にまで興味を示したが，主定理の証明の前に剰余体 $\mathbb{Z}/(5)$ や複素数体 $\mathbb{C}=\mathbb{R}[x]/(x^2+1)$ を扱ったところ，「分からない」，「分かりにくい」との声が上がり，幾度も説明を重ねることになった。

そうした経緯に加えて，生徒の分かりたいとの思いがあったのであろう，1週間後には単拡大の話が大体分かると発言する者も2，3名現れた。

その2，3名は最後までついてきて，「どうしても知りたかったことが分かって感動した。しかし，置換群がうまく利用されるとは全く予想できなかった。」との感想を述べてくれた。

毎回の講義を準備しながら，高校生に理解できる説明が可能だろうかと迷ったが，高木先生の説明を補ったり，例を加えたりしつつ主定理にたどりつけたときの満足感は生徒に劣らないであろう。

アーベル生誕200年の年にこのような講義ができ，意欲ある高校生の理解力のすごさに接する機会が与えられたことに感謝するとともに，体の拡大等の分

かりやすい説明法について考察を加え，方程式論がより身近なものになるよう工夫したいと思う。

参 考 文 献

1) 服部 昭著「現代代数学」朝倉書店（昭和47年）
2) 高木貞治著「代数学講義」共立出版（2002年）
3) 永田雅宜著「可換体論」裳華房（昭和60年）
4) 松坂和夫著「代数系入門」岩波書店（1994年）