富山大学教育学部紀要B（理科系）No.41：1－8（平成四年）

代数方程式論（II）

浅沼照雄

（1992年1月9日受理）

A Theory of Algebraic Equations (II)

Teruo ASANUMA

はじめに

本稿は代数方程式論（I）〔(2)〕に続くものである。5次の代数方程式の代数的解法が一般的には不可能であることの，ルフィニ，アーベル等のアイデアによる，初等的な証明を完結させるとともに，実際に前稿及び本稿を，セミナーを通して，本学部の三，四年次学生の指導に用いて得られた教育上の問題点等についても考察を加える。

前稿，代数方程論（I）の目次をあげておく。

以下本稿に続く。

7．置換についての注意

ここでは，ルファニ，アーベルの理論に必要な置換についての事柄について述べる。前稿同様にここでの置換とは，5文字｛1，2，3，4，5｝の置換のことである。

命題1．　任意の（5文字の）偶置換は，3次の巡回置換の積で表わせる。

証明．　2つの互換の積が3次の巡回置換の積で表わせればよい。任意の2つの互換を

$$\sigma=(ij),\ \tau=(km)$$

とする。ここでi，j，k，mは1，2，3，4，5のいずれかの数字でi≠j，k≠mとする。すると次の3つの場合が考えられる。

（I）　i，j，k，mがすべて異なるとき。

このときは

$$\sigma\tau=(ijk)(jkm)$$

とすればよい。

（II）　i，j，k，mの中で一組が等しいとき

このときは，j=kとしてよい。なぜならば，i=kのときはiをjに，jをiにあらためておきなおせばよい。他の場合も同様な操作をして，始めからj=kと仮定してよい。すると

$$\sigma\tau=(ij)(jm)=(ijm)$$

となり，この場合もなりたつ。

（III）　i=k，j=mのとき。

このときは

$$\sigma\tau=(1)=\text{恒等置換}$$

であるから

$$\sigma\tau=(123)^3$$

とすればよい。　（証明終）

命題2．　任意の（5文字の）偶置換は5次の巡回置換の積で表わせる。

証明．　命題1より任意の偶置換は3次の巡回置換の積で表わされるから，任意の3次の巡回置換が5次の巡回置換の積で表わされることを示せばよい。実際

$$(ijk)=(imknj)(minkj)$$

である。ここでi, j, k, m, nは1から5までのすべての文字を表わす。　（証明終）

8．不可能の証明

本節では以上の準備の下で，本稿の目的の一つである次の定理を証明する。

定理．　5次の代数方程式の代数的解法は一般には不可能である。

証明．　x_1, x_2, x_3, x_4, x_5を不定元として，これらを根にもつ5次方程式

$$\begin{aligned} f(x)&=(x-x_1)(x-x_2)(x-x_3)(x-x_4)\\ &\quad (x-x_5)\\ &=x^5-X_1x^4+X_2x^3-X_3x^2+X_4x-X_5\\ &=0 \end{aligned} \tag{1}$$

を考える。前稿第5節で述べたように，もし方程式(1)に代数的な解が存在するならば（P_1），（P_2）をみたす$\Phi_1,\cdots,\Phi_n$が存在して

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

とできる。ここで$K=\mathbf{C}(X_1,\cdots,X_5)$である。更に同節のアーベルの補題より$\Phi_1,\cdots,\Phi_n$は複素係数の$x_1$, x_2, x_3, x_4, x_5を不定元とする有理式と仮定できる。アーベルの補題は次節で証明する。あるiについてΦ_iが$K(\Phi_1,\cdots,\Phi_{i-1})$の元ならば

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

がなりたつから，始めからすべてのi＝1，…，nについて

$$\Phi_i\notin K(\Phi_1,\cdots,\Phi_{i-1})$$

としてもよい，上の式においてi＝1のときは

$$\Phi_1\notin K$$

と考える。

（注．$K\neq\mathbf{C}(x_1,\cdots,x_5)$であるから，上のような$\Phi_i$が，5次の方程式には代数的解法が存在するという仮定の下で，かならず存在することに注意しておく。）

そこで，まず第一にΦ_1を考えてみよう。仮定よりΦ_1は複素数を係数にもつ$x_1,\cdots,x_5$の有理式であるから

$$\begin{aligned}\Phi_1&=\Phi_1(x_1,x_2,x_3,x_4,x_5)\\ &=\Phi_1(x_1,\cdots,x_5)\end{aligned}$$

と表わす。

$$\Phi_1\notin K=\mathbf{C}(X_1,\cdots,X_5)$$

ゆえΦ_1は対称ではない

（注．対称有理式は第6節で見たように，対称式の商で表わされ，対称式は基本対称式の整式で表わされる。ゆえにΦ_1が対称有理式であるとすると$X_1,\cdots,X_5$の有理式となり$\Phi_1\notin K$なる仮定に矛盾する。）

ゆえにある互換σが存在して${}^{\sigma}\Phi_1\neq\Phi_1$とできる。一方，$p_1=p$とおくと，仮定より$\Phi_1^p\in K$，すなわち$\Phi_1^p$は対称有理式であるから

$${}^{\sigma}(\Phi_1^p)=\Phi_1^p$$

がなりたつ。明らかに

$${}^{\sigma}(\Phi_1^p)=({}^{\sigma}\Phi_1)^p$$

であるから

$$({}^{\sigma}\Phi_1)^p=\Phi_1^p$$

を得る。すなわち　${}^{\sigma}\Phi_1$は$\varepsilon(\neq1)$を1つのp乗根として

$${}^{\sigma}\Phi_1=\varepsilon\Phi_1$$

と表わせる。ゆえ

$$\Phi_1{}^{\sigma\sigma}\Phi_1=\varepsilon\,{}^{\sigma}\Phi_1=\varepsilon^2\Phi_1$$

であり，これにより$\varepsilon=-1$となる。すなわち$p_1=p=2$となる。

以上のことより　$\Phi_1=\Phi_1(x_1,\cdots,x_5)$は第6節の系2の条件をみたす。ゆえに有理対称式Gが存在して$\Phi_1=G\Delta$と表わせる。ここでΔは$x_1,\cdots,x_5$の差積である。

さてGは有理対称式であるから前に述べたように$G\in K$。ゆえに

$$K(\Phi_1)=K(\Delta)$$

がなりたつ。なぜならば$K(\Phi_1)$は体であるから

$$G^{-1}\in K(\Phi_1)$$

更に

$$G^{-1},\ \Phi_1\in K(\Phi_1)\Rightarrow\Delta=G^{-1}\Phi_1\in K(\Phi_1)$$

がなりたつからである。ゆえにΦ_1のかわりにΔを考えればよい。そこで始めからΦ_1をΔとおい

てよい。すなわち5次方程式に代数的な根の公式が存在すると仮定すると，$D=\Delta^2(\in K)$ とおいて $\sqrt{D}$ なる形の2乗根がかならず現われる。

次に第二の元，Φ_2について考える。仮定より Φ_2は $K(\Phi_1)$ に入らない $x_1,\cdots,\ x_5$の有理式である。そこでσを任意の偶置換として ${}^{\sigma}\Phi_2=\Phi_2$ とすると，第6節の系3より，有理対称式 F_1，F_2が存在して

$$\Phi_2=F_1+F_2\Delta$$

と表わせる。ところで F_1，F_2は K の元であるから

$$\Phi_2=F_1+F_2\Delta\in K(\Delta)=K(\Phi_1)$$

となり仮定に矛盾する。すなわち ${}^{\tau}\Phi_2\neq\Phi_2$ なる偶置換τが存在する。一方，命題1よりτは3次の巡回置換の積であるから，そのうちの少なくとも一つ，それを α とする，について ${}^{\alpha}\Phi_2\neq\Phi_2$ となる。

（注．τは3次の巡回置換 $\alpha_1,\cdots,\ \alpha_m$の積

$$\tau=\alpha_1\cdots\alpha_m$$

とすると，ある $\alpha=\alpha_j$について

$${}^{\alpha}\Phi_2\neq\Phi_2$$

となる。なぜならば，もしすべての α_i(i=1,…, m) について

$${}^{\beta}\Phi_2=\Phi_2(\beta=\alpha_i)$$

とすると

$${}^{\tau}\Phi_2=\Phi_2$$

となって矛盾を生ずる。）

そこで $p_2=q$ とおくと仮定より

$$\Phi_2^{\,q}\in K(\Phi_1)=K(\Delta)$$

がなりたつ，ゆえに

$$\Phi_2^{\,q}=a_0+a_1\Delta(a_0,a_1\in K)$$

と表わせる。3次の巡回置換は偶置換なることに注意すれば，a_0，a_1は対称有理式，Δは交代式ゆえ

$${}^{\alpha}(a_0+a_1\Delta)=a_0+a_1\Delta$$

であるから

$$({}^{\alpha}\Phi_2)^q={}^{\alpha}(\Phi_2^{\,q})=\Phi_2^{\,q}$$

がなりたつ，それゆえにεを1のq乗根とすれば

$${}^{\alpha}\Phi_2=\varepsilon\Phi_2$$

と表わせる。αは3次の巡回置ゆえ $\alpha^3=(1)=$恒等置換となるから

$$\begin{aligned}\Phi_2&={}^{\alpha\alpha\alpha}\Phi_2={}^{\alpha\alpha}(\varepsilon\Phi_2)\\&=\varepsilon\,{}^{\alpha\alpha}\Phi_2=\varepsilon\,{}^{\alpha}(\varepsilon\Phi_2)\\&=\varepsilon\,{}^{2\alpha}\Phi_2=\varepsilon^3\Phi_2\end{aligned}$$

を得る。これより $\varepsilon^3=1$．更に

$$\varepsilon\Phi_2={}^{\alpha}\Phi_2\neq\Phi_2$$

より $\varepsilon\neq1$，すなわちεは1の虚3乗根となる。それゆえ　q=3である。

さて，こんどは命題2よりτは5次の巡回置換の積と表わせる。それゆえ3次の場合とはまったく同様にして5次の巡回置換βが存在して

$${}^{\beta}\Phi_2\neq\Phi_2$$

と表わせる。3次の場合と同様の議論を適用して q=5 を得るが，これは上記の結果 q=3 に矛盾する。すなわち定理が証明された。　（証明終）

9．アーベルの補題の証明

前節において，5次の代数方程式の代数的解法は不可能であることが証明されたが，これは前稿第5節のアーベルによる補題を仮定していた。この節ではそれを証明する。アーベルの原論文〔(1)〕のままでは不十分である。守屋［(1), p.54-56］において，拡大体の次数の理論を用いてその厳密な証明をしているが，本論文の教育目的にそぐわない。以下，アーベルのアイデアに基づいた初等的な証明を試みる。

さてアーベルの補題を再記すると，次のようなものであった。

X_i(i=1,…, 5) は不定元 x_1，x_2，x_3，x_4，x_5 のi次の基本対称式とし，$K=\mathbf{C}(X_1,\cdots,X_5)$ 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（複素係数）とすることができる。

証明．　仮定より $x_i\in K(\Phi_1,\cdots,\Phi_n)$(i=1,…,5) である。nをこのような仮定をみたす最小の数としておく。

（注．アーベルの補題の仮定をみたす $\Phi_1,\cdots,\ \Phi_n$の中で，nが最小となるように $\Phi_1,\cdots,\ \Phi_n$を選んでおく。）

明らかに $n \geqq 1$ である。さて $x_i\ (i=1, \cdots, 5)$ は

$$x_i = a_{i0} + a_{i1}\Phi_n + \cdots + a_{ip-1}\Phi_n^{p-1}$$

$(p=p_n,\ a_{ij} \in K(\Phi_1, \cdots, \Phi_n) j=0,1, \cdots, p-1)$

と表わせる。ここで $a_{i0}(j=1, \cdots, 5)$ 以外の a_{ij} がすべて 0 とすると

$$x_i = a_{i0} \in K(\Phi_1, \cdots, \Phi_{n-1})$$

となり n の最小性の仮定に反する。ゆえに a_{ij} $(j \neq 0)$ の少なくとも 1 つは 0 でないことに注意しておく。

さて $a_{ij}(i=1, \cdots 5,\ j=0, \cdots, p-1)$ 及び Φ_n^p よりなる集合を A とおく，すなわち

$$A = \{a_{ij}, \Phi_n^p | j=1, \cdots, 5, j=0,1, \cdots, p-1\}$$

である。A の任意の元 $a(=a_{ij}$ 又は $\Phi_p)$ は $K(\Phi_1, \cdots, \Phi_{n-1})$ の元であるから

$$a = b_{a0} + b_{a1}\Phi_{n-1} + \cdots + b_{aq-1}\Phi_{n-1}^{q-1}$$

$(q=p_{n-1}, b_{aj} \in K(\Phi_1, \cdots, \Phi_{n-2}), j=0, \cdots, q-1)$

と表わされる。もしすべての A の元 a について $b_{aj}(j=1, \cdots, q-1)$ が 0 ならば

$$a = b_{a0} \in K(\Phi_1, \cdots, \Phi_{n-2})$$

となる。とくに $a=\Phi_n^p$ のときを考えると

$$\Phi_n^p \in K(\Phi_1, \cdots \Phi_{n-2})$$

がなりたつ。ゆえ

$$K \subset K(\Phi_1) \subset \cdots \subset K(\Phi_1, \cdots, \Phi_{n-2}) \subset K(\Phi_1, \cdots \Phi_{n-2}, \Phi_n)$$

は (P_1), (P_2) をみたし

$$x_i \in K(\Phi_1, \cdots, \Phi_{n-2}, \Phi_n)\ (i=1, \cdots, 5)$$

がなりたつ。これは $\Phi_1, \cdots, \Phi_n$ の個数に関する最小性の仮定に反する。ゆえにある $a \in A$ が存在して $b_{a1}, b_{a2}, \cdots, b_{aq-1}$ の中の少なくとも 1 つは 0 ではない。

さてすべての $b_{aj}(a \in A,\ j=0,1, \cdots, q-1)$ 及び

Φ_{n-1}^q よりなる集合を B で表わす，すなわち

$$B = \{b_{aj}, \Phi_{n-1}^q | a \in A,\ j=0,1, \cdots, q-1\}$$

である。B の任意の元 $b(=b_{aj}$ 又は $\Phi_{n-1}^q)$ は $K(\Phi_1, \cdots, \Phi_{n-2})$ の元であるから

$$b = c_{b0} + c_{b1}\Phi_{n-2} + \cdots c_{br-1}\Phi_{n-2}^{r-1}$$

$(r=p_{n-2}, c_{bj} \in K(\Phi_1, \cdots, \Phi_{n-3}), j=0,1, \cdots, r-1)$

と表わせる。前とまったく同様の議論を繰返してある $b \in B$ が存在して $c_{b1}, \cdots c_{br-1}$ の中の少なくとも 1 つは 0 でない。

さてすべての $c_{bj}(b \in B,\ j=0,1, \cdots,\ r-1)$ 及び Φ_{n-2}^r よりなる集合を C で表わす。すなわち

$$C = \{c^{bj},\ \Phi_{n-2}^r | b \in B,\ j=0,1, \cdots,\ r-1\}$$

である。

以下同様にして集合 D,E,… を定義する。以上をまとめて整理すると，集合 A, B, C, D, E, …は

$$A \subset K(\Phi_1, \cdots, \Phi_{n-1})$$
$$B \subset K(\Phi_1, \cdots, \Phi_{n-2})$$
$$C \subset K(\Phi_1, \cdots, \Phi_{n-3})$$
$$D \subset K(\Phi_1, \cdots, \Phi_{n-4})$$
$$E \subset K(\Phi_1, \cdots, \Phi_{n-5})$$
$$\vdots$$

であって，A については

$$A = \{a_{ij}, \Phi^p{}_n | i=1, \cdots, 5, j=0,1, \cdots, p-1\} \qquad (p=p_n)$$

$$x_i = a_{i0} + a_{i1}\Phi_n + \cdots + a_{ip-1}\Phi_n^{p-1} \qquad (i=1, \cdots, 5)$$

とくに $a^{ij} \neq 0$ $(j \neq 0)$ なる元が存在する。

又 B については

$$B = \{b^{aj}, \Phi_{n-1}^q | a \in A, j=0,1, \cdots, q-1\} \qquad (q=p_{n-1})$$

$$a = b_{a0} + b_{a1}\Phi_{n-1} + \cdots + b_{aq-1}\Phi_{n-1}^{q-1} \qquad (a \in A)$$

とくに $b_{aj} \not\equiv 0$ $(j \neq 0)$ なる元が存在する。

又 c については

$$C = \{c_{bj},\ \Phi_{n-2}^r | b \in B,\ j=0,1, \cdots,\ r-1\} \qquad (r=p_{n-2})$$

$$b = c_{b0} + c_{b1}\Phi_{n-2} + \cdots + c_{bq-1}\Phi_{n-1}^{r-1} \qquad (b \in B)$$

とくに $c_{bj} \not\equiv 0$ $(j \neq 0)$ なる元が存在する。

以下同様に C, D, E,… が定義されている。ゆえに集合の A, B, C, D, E, … の最後を Z とおくと Z は K の部分集合となる。

さて以上の準備の下に，$\Phi_1, \cdots, \Phi_n$ をうまく選ぶことによって $\Phi_1, \cdots, \Phi_n$ が $x_1, \cdots, x_5$ の複素係数の有理式とできることを示そう。

まず第一段として Φ_n をうまくえらぶことにより Φ_n 及び A のすべての元が $x_1, \cdots,\ x_5$ の有理式となるようにできることを示す。

始めに第一のステップとして

$$a_{i0}, a_{i1}\Phi_n, a_{i2}\Phi_n^2, \cdots, a_{ip-1}\Phi_n^{p-1} (i=1, \cdots, 5)$$

がすべて $x_1, \cdots,\ x_5$ の有理式であることを示す。

そこで

$$F_i(X)=a_{i0}+a_{i1}X+\cdots+a_{ip-1}X^{p-1}$$

とおく

$$f(x)=x^5-X_1x^4+X_2x^3-X_3x^2+X_4x-X_5$$
$$=(x-x_1)(x-x_2)(x-x_3)(x-x_4)$$
$$(x-x_5)$$

であったから $f(x_i)=0$ に注意する。他方この $f(x)$ に $x=F_i(X)$ を代入すると

$$f(F_i(X))=F_i(X)^5-X_1F_i(X)^4+\cdots+X_4F_i(X)-X_5$$

であり，これは簡単な計算により $K(\Phi_1,\cdots,\Phi_{n-1})$ を係数にもつ変数 X の多項式である。すなわち

$$f(F_i(X))=G(X)=A_0X^m+A_1X^{m-1}+\cdots+A_m$$
$$(A_i\in K(\Phi_1,\cdots,\Phi_{n-1}))$$

と表わせる。そこで任意の正の整数 j について j を p で割った商 $Q(j)$，余りを $R(j)$ で表わすことにすると

$$j=Q(j)p+R(j)\quad(0\leqq R(j)<p)$$

であるから

$$G(X)=A_0X^{Q(m)p+R(m)}+A_1X^{Q(m-1)p+R(m-1)}+\cdots+$$
$$A_{m-1}X+A_m$$

となる。それゆえ $G(X)$ は

$$G(X)=G_1(X^p)X^{p-1}+\cdots+G_{p-1}(X^p)X+$$
$$G_p(X^p)$$

と表わせる。ここで $G_j(X)$ は $K(\Phi_1,\cdots,\Phi_{n-1})$ に係数をもつ変数 X の多項式で $G_j(X^p)$ はその X に X^p を代入したものである。それゆえ $G_j(X^p)$ の X に Φ_n を代入した値 $G_j(\Phi_n^p)$ は $K(\Phi_1,\cdots,\Phi_{n-1})$ の元となる。さて $G(X)$ に Φ_n を代入すると

$$G(\Phi_n)=G_1(\Phi_n^p)\Phi_n^{p-1}+\cdots+G_{p-1}(\Phi_n^p)\Phi_n+$$
$$G_p(\Phi_n^p)$$

と表わされる。仮定より

$$G(\Phi_n)=f(F_i(\Phi_n))=f(x_i)=0$$

であるから，$\Phi_n\notin K(\Phi_1,\cdots,\Phi_{n-1})$ に注意すれば，前稿第4節（P_3）より

$$G_1(\Phi_n^p)=G_2(\Phi_n^p)=\cdots=G_p(\Phi_n^p)=0$$

となる。そこで ε を1の任意の p 乗根とすると，

$$G(\varepsilon\Phi_n)=G_1(\Phi_n^p)\ \varepsilon^{p-1}\Phi_n^{p-1}+\cdots+$$
$$G_{p-1}(\Phi_n^p)\varepsilon\Phi_n+G_p(\Phi_n^p)=0$$

であるから

$$f(F_i(\varepsilon\Phi_n))=G(\varepsilon\Phi_n)=0$$

がなりたつ。すなわち $F_i(\varepsilon\Phi_n)$ は $f(x)=0$ の根である。それゆえ $F_i(\varepsilon\Phi_n)$ は $x_1,\cdots,x_5$ のどれかと等しい，とくに $F_i(\varepsilon\Phi_n)$ は $x_1,\cdots,x_5$ の有理式である。まったく同様にして任意の $j=1,\cdots,p-1$ について $F_i(\varepsilon^j\Phi_n)$ が $x_1,\cdots,x_5$ の有理式であることが示される。一方

$$F_i(\Phi_n)=a_{i0}+a_{i1}\Phi_n+\cdots+a_{ip-1}\Phi_n^{p-1}$$
$$F_i(\varepsilon\Phi_n)=a_{i0}+a_{i1}\varepsilon\Phi_n+\cdots+a_{ip-1}\varepsilon^{p-1}\Phi_n^{p-1}$$
$$\vdots$$
$$F_i(\varepsilon^{p-1}\Phi_n)=a_{i0}+a_{i1}\varepsilon^{p-1}\Phi_n+\cdots+$$
$$a_{ip-1}\varepsilon^{(p-1)(p-1)}\Phi_n^{p-1}$$

より，$\varepsilon\neq1$ のときこの連立方程式を

$$a_{i0},\ a_{i1},\cdots,\ a_{ip-1}\Phi_n^{p-1}$$

について解くと，

$$a_{i0}=\frac{1}{p}(y_0+y_1+\cdots+y_{p-1})$$

$$a_{i1}\Phi_n=\frac{1}{p}(y_0+\varepsilon^{-1}y_1+\cdots+\varepsilon^{-(p-1)}y_{p-1})$$

$$\vdots$$

$$a_{ip-1}\Phi_n^{p-1}=\frac{1}{p}(y_0+\varepsilon^{-(p-1)}y_1+\cdots+$$
$$\varepsilon^{-(p-1)(p-1)}y_{p-1})$$

を得る。ここで $y_j=F_i(\varepsilon^j\Phi_n)$ である。

（注．$1+\varepsilon+\varepsilon^2+\cdots+\varepsilon^{p-1}=0$ をもちいていることに注意すればよい。）

$y_0,\ y_1,\cdots,\ y_{p-1}$ は $x_1,\cdots,x_5$ の有理式であったから

$$a_{i0},\ a_{i1}\Phi_n,\cdots,\ a_{ip-1}\Phi_n^{p-1}$$

もすべて $x_1,\cdots,x_5$ の有理式となり第一のステップが示された。

次に第二のステップとして，Φ_n をうまく選んである k（$0\leqq k\leqq5$）に対して

$$x_k=a_{k0}+\Phi_n+a_{k2}\Phi_n^2+\cdots+a_{kp-1}\Phi_n^{p-1}$$
$$(a_{k0},\ a_{k2},\cdots,\ a_{kp-1}\in K(\Phi_1,\cdots,\Phi_{n-1}))$$

と表わせることを示そう。すなわち A の元 a_{ij} について $a_{k1}=1$ とできることを示す。

仮定により $a_{kj}\neq0$（$j\neq0$）なる元 a_{kj} が A に存在する。$a_{k1},\ a_{k2},\cdots,\ a_{kp-1}$ の最初に0にならない元を a_{kj} とすると

$$x_k=a_{k0}+a_{kj}\Phi_n^j+\cdots+a_{kp-1}\Phi_n^{p-1}\qquad(2)$$

と表わせる。さてpは素数であって，jはpより小さい正の整数であるからjとpは互いに素である。ゆえに $j\lambda+p\nu=1$ をみたす整数の組 λ，ν が存在する。α を任意の正の整数としてこの両辺にかけると

$$j\lambda\alpha+p\nu\alpha=\alpha$$

である。さらに $\lambda\alpha$ をpで割った商 $Q(\lambda\alpha)$ を β，余り $R(\lambda\alpha)$ を γ とおくと

$$\lambda\alpha=\beta p+\gamma\ (0\leqq\gamma<p)$$

であるから，これを上の式に代入して

$$j(\beta p+\gamma)+p\nu\alpha=\alpha$$

がなりたつ。すなわち α はmod pで考えると

$$\alpha\equiv j\gamma(\mathrm{mod}\ p)\quad(0\leqq\gamma<p)$$

と表わせる。初等整数論より $\gamma=1$ なるための必要十分条件は $\alpha\equiv j(\mathrm{mod}\ p)$ なることに注意しておく。そこで

$$a_{kj}\Phi_n^{j}=\Phi$$

とおくと

$$\Phi^p=a_{kj}^{p}(\Phi_n^{p})^{j}\in K(\Phi_1,\cdots,\Phi_{n-1})$$

であり，かつ

$$\begin{aligned}\Phi_n^{\alpha}&=\Phi_n^{j(\beta+\gamma)+p\gamma\alpha}\\&=(\Phi^p)^{j\beta+\gamma\alpha}\Phi_n^{j\gamma}\\&=(\Phi^p)^{j\beta+\gamma\alpha}a_{kj}^{\gamma}\Phi^{\gamma}\end{aligned}$$

がなりたつ。更に

$$(\Phi^p)^{j\beta+\gamma\alpha}a_{kj}^{\gamma}=a_{\alpha}$$

とおけば $a_\alpha\in K(\Phi_1,\cdots,\Phi_{n-1})$ である。以上をまとめると

$$\Phi_n^{\alpha}=a_{\alpha}\Phi^{R(\lambda\alpha)}\quad(0\leqq R(\lambda\alpha)<p)\qquad(3)$$

がなりたち，

$$\alpha\equiv\alpha'(\mathrm{mod}\ p)\Leftrightarrow R(\lambda\alpha)=R(\lambda\alpha')$$

に注意すれば

$$R(\lambda j),\ R(\lambda(j+1)),\cdots,\ R(\lambda(p-1))$$

はすべて異なるp−1以下の正の整数である。ゆえに(3)を(2)に代入して得られた式

$$x_k=a_{kj}+a_j\Phi^{R(\lambda j)}+\cdots+a_{kp-1}a_{p-1}\Phi^{R(\lambda(p-1))}$$

は

$$a_{kj}a_j\Phi^{R(\lambda j)}=\Phi$$

であるから

$$x_k=a_{k0}+\Phi+a'_{k2}\Phi^2+\cdots+a'_{kp-1}\Phi^{p-1}$$

$$(a'_{k2},\cdots,\ a'_{kp-1}\in K(\Phi_1,\cdots,\ \Phi_{n-1}))$$

と表わせる。そこで

$$K(\Phi_1,\cdots,\ \Phi_{n-1},\Phi_n)=K(\Phi_1,\cdots,\Phi_{n-1},\Phi)$$

に注意して，始めから Φ を Φ_n とおけば

$$x_k=a_{k0}+\Phi_n+a_{k2}\Phi_n^{2}+\cdots+a_{kp-1}\Phi_n^{p-1}$$

と表わされ第二のステップが証明された。

さて第一段の証明に入る。

第一のステップより任意のi＝1，…，5について

$$a_{l0},\ a_{l1}\Phi_n,\cdots,\ a_{lp-1}\Phi_n^{p-1}$$

は $x_1,\cdots,\ x_5$ の有理式となる。特に第二ステップより

$$a_{k0},\ \Phi_n,\ a_{k2}\Phi^2,\cdots,\ a_{kp-1}\Phi_n^{p-1}$$

は $x_1,\cdots,\ x_5$ の有理式となる。ゆえ Φ_n は有理式となる。再び第一のステップより

$$a_{l0},\ a_{l1},\cdots,\ a_{lp-1}$$

が任意のi＝1，…，5について有理式となる。なぜならば任意の整数i，j(i＝1，…，5，j＝0，1，…，p−1)に対して $a_{ij}\Phi_n^{i}$ が有理式ならば Φ_n が有理式ゆえ a_{ij} も有理式になるからである。これで第一段に主張が証明された。

次に第二段として集合Bに対してもAと同様な事実がなりたつことを示す。すなわち Φ_{n-1} をうまく選んでBのすべての元，及び Φ_{n-1} が $x_1,\cdots,\ x_5$ の有理式となることを証明しよう。そこで第一段の証明と同様に，まず第一のステップとして任意の $a\in A$ について

$$b_{a0},\ b_{a1}\Phi_{n-1},\cdots,\ b_{aq-1}\Phi_{n-1}^{q-1}$$

が $x_1,\cdots,\ x_5$ の有理式となることを示そう。前に示したとおりAの任意の元aは $x_1,\cdots,\ x_5$ の有理式である。それゆえ

$$a=a(x_1,\cdots,\ x_5)=x_1,\cdots,x_5\text{の有理式}$$

と表わせる。

$$a_l={}^{\sigma}a(\sigma=\sigma_l)$$

とおく。ここに σ_l(i＝1，…，120) は {1, 2, 3, 4, 5} のすべての置換を表わす。σ_l は恒等置換としておく。ゆえ $a_1=a$ となる。そこで

$$g(X)=(X-a_1)(X-a_2)\cdots(X-a_{120})$$

とおく。すると根と係数の関係により

$$g(X)=X^{120}-s_1X^{119}+s_2X^{118}-\cdots+(-1)^{l}s_lX^{120-l}+\cdots+s_{120}$$

と表わせる。ここで s_l は $a_1,\cdots,a_{120}$ のi次の基本対称式である。さて一般にsを $a_1,\cdots,\ a_{120}$ の対称式とすると，sは $x_1,\cdots,x_5$ に関して対称有

理式になる。なぜならばτを$\{1, 2, 3, 4, 5\}$の任意の互換としたとき

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

であるから

$$\{\tau a_1, \tau a_2, \cdots, \tau a_{120}\}=\{a_1, a_2, \cdots, a_{120}\}$$

がなりたつ，そこで$s=S(a_1, a_2, \cdots, a_{120})$（$=a_1, a_2, \cdots, a_{120}$についての式）とおくと

$$^{\tau}s=S(^{\tau}a_1, ^{\tau}a_2, \cdots, ^{\tau}a_{120})$$

である。すなわち$^{\tau}s$は中に表われる$a_1, \cdots, a_{120}$を交換して得られる。ゆえに$^{\tau}s=s$となりsを$x_1, \cdots, x_5$の有理式と考えて対称になるが，前稿6節より対称式の商で表わせるから，sは$X_1, \cdots X_5$の有理式となる。ゆえに$s_1, \cdots, s_{120}$は$X_1, \cdots, X_5$の有理式，すなわち$K=\mathbf{C}(X_1, \cdots, X_5)$の元である。それゆえ方程式$g(X)=0$はKの元を係数にもつ$a_1, a_2, \cdots, a_{120}$を根とする120次の代数方程式である。

さて

$$H(X)=b_{a0}+b_{a1}X+\cdots+b_{ag-1}X^{g-1}$$

とおくと，$g(H(X))$は$K(\Phi_1, \cdots, \Phi_{n-2})$の元を係数にもつ変数Xの整数である。第一段の証明と同様にして$g(H(X))=L(X)$とおくと

$$L(X)=L_1(X^q)x^{q-1}+\cdots+L_{q-1}(X^q)x+L_q(X^q)$$

と表わせる。ここで$L_j(X)$は$K(\Phi_1, \cdots, \Phi_{n-2})$の元を係数にもつ変数Xの整式である。ところで

$a=H(\Phi_{n-1})$は方程式$g(X)=0$の根であるから

$$L(\Phi_{n-1})=L_1(\Phi_{n-1}^{q})\Phi_{n-1}^{q-1}+\cdots+L_q(_{n-1}^{q})=0$$

がなりたつ。

$$L_j(_{n-1}^{q})\in K(\Phi_1, \cdots, \Phi_{n-2})$$

及び

$$\Phi_{n-1}\notin K(\Phi_1, \cdots, \Phi_{n-2})$$

であるから，(P_3)が適用されて

$$L_1(\Phi_{n-1}^{q})=L_2(\Phi_{n-1}^{q})=\cdots=L_q(\Phi_{n-1}^{q})=0$$

を得る。さてεを1のq乗根すると

$$g(H(\varepsilon\Phi_{n-1}))=L(\varepsilon\Phi_{n-1})=0$$

であるから

$$H(\varepsilon\Phi_{n-1})=b_{a0}+b_{a1}\varepsilon\Phi_{n-1}+\cdots+b_{aq-1}\varepsilon^{q-1}\Phi_{n-1}^{q-1}$$

は$g(X)$の根となる。ゆえに$H(\varepsilon\Phi_{n-1})$は$a_1, \cdots, a_{120}$のどれかに等しい，すなわち$H(\varepsilon\Phi_{n-1})$は$x_1, \cdots, x_5$の有理式となる。まったく同様にして

$$H(\varepsilon^2\Phi_{n-1}), \cdots, H(\varepsilon^{q-1}\Phi^{n-1})$$

も$x_1, \cdots, x_5$の有理式となる。以上をまとめて

$$b_{a0}, b_{a1}\Phi_{n-1}, \cdots, b_{aq-1}\Phi_{n-1}^{q-1}$$

に関する連立方程式

$$H(\Phi_{n-1})=b_{a0}+b_{a1}\Phi_{n-1}+\cdots+b_{aq-1}\Phi_{n-1}^{q-1}$$

$$H(\varepsilon\Phi_{n-1})=b_{a0}+b_{a1}\varepsilon\Phi_{n-1}+\cdots+b_{aq-1}\varepsilon^{q-1}\Phi_{n-1}^{q-1}$$

$$\vdots$$

$$H(\varepsilon^{q-1}\Phi_{n-1})=b_{a0}+b_{a1}\varepsilon^{q-1}\Phi_{n-1}+\cdots+b_{aq-1}\varepsilon^{(q-1)(q-1)}\Phi_{n-1}^{q-1}$$

を得る。これを$\varepsilon\neq 1$のとき第一段と同様に解いて$b_{a0}, b_{a1}\Phi_{n-1}, \cdots, b_{aq-1}\Phi_{n}^{q-1}$が$x_1, \cdots, x_5$の有理式となることが示される。

次に第二のステップとして，Φ_{n-1}をうまく選んであるa∈Aに対して

$$a=b_{a0}+\Phi_{n-1}+b_{a2}\Phi_{n-1}^{2}+\cdots+b_{aq-1}\Phi_{n-1}^{q-1}$$

$$(b_{a0}, b_{a2}, \cdots, b_{aq-1}\in K(\Phi_1, \cdots, \Phi_{n-2}))$$

と表わせることを示すのであるが，証明は第一段の第二のステップとまったく同様にしてできるので略す。

さてこの第一及び第二のステップより第二段の主張は第一段のときと同様に示される。

以下同様の議論を集合C, D, E, …, Zについておこなうことによって，とくに$\Phi_n, \Phi_{n-1}, \cdots, \Phi_1$を$x_1, \cdots, x_5$の有理式なるように選ぶことができる

（証明終）

10: 学部教育における代数方程式論

前稿及び本稿の第9節までの原稿をもとに，卒業研究の一環として，本学部の3年次及び4年次の学生にセミナーをしてもらった。3年次の学生は2名で週一回，4年次の学生は5名で週二回の割合でセミナーを行った。予備知識としては〔(3)〕のみを仮定した。

まず前稿の第1節，第2節は問題がない。

第3節はもっとも基本的な節で，いわゆる体の概念が導入されているが，ここでは後の証明に必要な具体的な体，すなわち複素数体上の5変数の

有理函数体と，その上の巡回拡大体のみに限定した。

前稿注1にも述べたように，この節には論理的な前後が存在する。すなわち

$$K(\phi^{1/p}) \ni \Phi(\neq 0) \Rightarrow K(\phi^{1/p}) \ni \Phi^{-1}$$

を証明するところで

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

として，$G' \in K$ であると主張しているが，これは次に現われている補題

$\phi^{1/p} \notin K$, $\Phi=a_0+a_1\phi^{1/p}+\cdots+a_{p-1}\phi^{(p-1)/p}=0$

$(i=0,\cdots, P-1) \Rightarrow a_i=0$ $(i=0,\cdots, p-1)$

を用いて $G' \neq 0$ を示す。

ゆえ指導上この点に特に注意してほしい。ただ教育的には，始めは $G' \neq 0$ なることを注意するにとどめ，補題を証明した後，その理由を説明するほうが，体の概念がストレートに出てくるだけ，初学者にはわかりやすいようである。

第4節は前3節にくらべ，やや難かしいようである。具体的に，たとえば体の拡大

$$K \subset K(\phi^{1/2}) \subset K(\phi^{1/2}, \psi^{1/3})$$

について K の任意の元 Φ が

$$\Phi=a_{00}+a_{01}\phi^{1/2}+a_{10}\psi^{1/3}+a_{11}\phi^{1/2}\psi^{1/3}+a_{20}\psi^{2/3}+a_{21}\phi^{1/2}\psi^{2/3} \quad (a_{ij} \in K)$$

と表わせる等々，を用いてイメージをつかむようにするのも一つの方法であると思う。

第5節では次の事実を仮定している。すなわち $x_1, \cdots, x_5$ が不定元としたとき，その基本対称式 $X_1, \cdots, X_5$ は複素数体上代数的に独立であるということである。厳密に述べると，$X_1, \cdots, X_5$ は代数的に独立（複素数体上）であるから，体 $\mathbf{C}(X_1, \cdots, X_5)$ は複素数体上5変数の有理函数体 $\mathbf{C}(x_1, \cdots, x_5)$ と同型となり，前節までの結果を，$X_1, \cdots, X_5$ を不定元とみることによって，用いることができる。しかし教育上の観点から見ると，$\mathbf{C}(X_1, \cdots, X_5)$ を同型を通して有理函数体と考えるのは，初学者にとっては少し難かしいようである。むしろ初めはその注意ぬきで，$X_1, \cdots, X_5$ を不定元として扱かい，体の概念になれてきた後に，あらためてその事実を指導するようにしたほうが効果は大きいようである。この第5節の理解が指導上のキイポイントであった。すなわち，アーベルの補題を仮定すれば，第6節から第8節までほとんど問題がなく，比較的わかりやすいようである。

第9節のアーベルの補題の証明については，当初アーベルの論文の引き写しでセミナーを行ったが，その中に論理展開が不十分な所があるため，学生の理解を得るには至らなかった。そこで本稿のように変更を加え，できるかぎり初学者の理解を得るようにしたが，結果は良好であった。

以上より第9節のアーベルの補題を仮定すれば比較的短期に，当初の目的を得られると思う。又上に見たとおり，アーベルの補題も初等的なものであり，いわゆる抽象的なガロア理論を指導する前，又は一般的な体の定義と，その簡単な性質を講義した後，このような古典的な理論を紹介する教育的効果は大きいと思う。

最後に前稿及び本稿には演習問題がないが，適当な演習問題を随時はさむのは是非とも必要であり，又一般の素数 p, q, …等について証明されている定理その他について，$p=2, 3, q=2, 3, \cdots$ 等々小さな素数についてできるかぎり確かめることも効果がある。

参考文献

(1) N.H. Abel, Beweis der Unmöglichkeit algebraiche Gleichungen von höheren Graden als dem vierten allgemein aufzulösen, Journal für die reine und angewandte Mathematik, vol 1, (1826) 62-84.
（日本語訳及び解説）
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

(2) 浅沼照雄　代数方程式論（I）　富山大学教育学部紀要（B理科系）第40号 (1992) 1-10.

(3) 淡中忠郎，代数学 (1964) 朝倉書店