# 高校生に5次方程式の解の公式が存在しないことを教える試み

理工学部 数学科　金沢雄太

2008年2月21日

## 1　はじめに

大学で数学を勉強するとき必ず触れる定理に、代数学の基本定理がある。

**定理 1.1 (代数学の基本定理)** [1] $n > 0, a_i \in \mathbb{C}\ (i = 1, 2, \ldots, n)$ とする。このとき、方程式

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

は必ず重複を考慮して $n$ 個の解をもつ。

この定理によって、どんな一変数の代数方程式も必ず解があることが保証されている。しかしその解が、方程式の係数の加減乗除と冪根の組み合わせで書き表す (解の公式) ことができるかどうかは200年以上不明であった。この問題は、ガロア理論[2]によって解決した。解の公式は、$n \leq 4$ のとき存在し、$n \geq 5$ のとき存在しないことがわかっている。

この論文で、$n = 5$ の場合に解の公式が存在しないことを高校生に教えることを試みる。しかし、厳密な証明を与えるとすると、やはり大学の知識を使わなければならない。

以下、5次方程式の解の公式が無いことを証明するための準備を行う。

この卒論では、木村俊一著「天才数学者はこう解いた、こう生きた：方程式四千年の歴史」(講談社) を深く参考にさせていただきました。

---

[1] 代数学の基本定理は17世紀前半にアルベール・ジラール (Albelt Girard) らにより主張され、多くの数学者が証明を試みた。ヨハン・カール・フリードリヒ・ガウス (Johann Carl Friedrich Gauss)(1777年～1855年：独) が1799年に、最初の完全な証明を与えた。

この定理により、実数係数の多項式は、必ず有限個の一次式と二次式の積の形に因数分解できることが示される。

[2] エヴァリスト・ガロア (Évariste Galois)(1811年～1832年：仏) により1829年に発見された。ガロア理論は、代数方程式や体の構造を“ ガロア群 ”と呼ばれる群を用いて記述する理論である。現在、ガロア理論に関する考え方は、数学、物理、コンピューターなどのあらゆる分野に現れている。

# 2　対称式論

5 次方程式の解の公式の非存在証明には、対称式という概念が必要になる。まず基本対称式を定義する。

**定義 2.1 (基本対称式)** $a_1, a_2, \ldots, a_n$ を $n$ 個の変数とする。$a_1, a_2, \ldots, a_n$ の中から $k$ 個 $(k \leq n)$ ずつペアを作って、掛け合わせてそれらの和をとった式を $k$ 次基本対称式という。

**例 2.2** $a, b, c, d$ を 4 個の変数とする。このとき、
1 次基本対称式: $a + b + c + d$
2 次基本対称式: $ab + ac + ad + bc + bd + cd$
3 次基本対称式: $abc + abd + acd + bcd$
4 次基本対象式: $abcd$
である。

つぎに、方程式の係数が、方程式の解の基本対称式で書き表せることを示す。いわゆる、方程式の解と係数の関係である。

**定理 2.3 (ジラールの定理)** [3]　方程式

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

の $n$ 個の解を、$\alpha_1, \alpha_2, \ldots, \alpha_n$ とする。このとき、

$$a_k = (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k}$$

が成り立つ。

**証明** $\alpha_1, \alpha_2, \ldots, \alpha_n$ が複素係数モニック多項式 $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ の根であるので、

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

と因数分解できる。右辺を展開するとき、一般に $x^{n-k}$ の係数は、$\alpha_1, \alpha_2, \ldots, \alpha_n$ から任意に $k$ 個選びそれらを掛けたものの全ての和であるから、

$$a_k = (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k}$$

が成り立つ。　**証明終**

この定理によって、複素係数モニック多項式 $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ の $k$ 次の係数は、その根の $k$ 次基本対称式の $(-1)^k$ 倍であることが分かった。

[3] アルベール・ジラール (Albelt Girard)(1595〜1632:仏)
1625 年にジラールの定理 (解と係数の関係) を発表した。ジラールは、初めて三角関数の sin, cos, tan という記号を用いた。また、正の方向と反対に進めば、それは負の方向を表すという概念を考えて、「負の数」の幾何学的解釈を行った。

**定義 2.4 (対称式)** $x_1, x_2, \ldots, x_n$ の任意の入れ替え $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ に対して

$$f(x_1, x_2, \ldots, x_n) = f(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$$

が成立するとき、$n$ 変数多項式 $f(x_1, x_2, \cdots, x_n)$ は $x_1, x_2, \ldots, x_n$ に関する対称式であるという。

**例 2.5** 基本対称式は対称式である。

$x, y, z$ に関する基本対称式を考える。変数 $x, y, z$ の入れ替えを全て書くと、$xyz$, $xzy$, $yxz$, $yzx$, $zxy$, $zyx$ の 6 つが出て来る。

$x, y, z$ の *1* 次基本対称式にこれらの入れ替えを施すと、

$$\begin{aligned}
x+y+z &\xrightarrow{xyz} x+y+z \\
x+y+z &\xrightarrow{xzy} x+z+y = x+y+z \\
x+y+z &\xrightarrow{yxz} y+x+z = x+y+z \\
x+y+z &\xrightarrow{yzx} y+z+x = x+y+z \\
x+y+z &\xrightarrow{zxy} z+x+y = x+y+z \\
x+y+z &\xrightarrow{zyx} z+y+x = x+y+z
\end{aligned}$$

となり、これらの入れ替えで $x+y+z$ は不変であることがわかった。同様にして、2 次, 3 次基本対称式も $xyz$ の入れ替えで不変であることが分かる。

ここで、対称式に関する最も重要な定理を述べる。

**定理 2.6 (対称式の基本定理)** $n$ 変数多項式 $f(x_1, x_2, \cdots, x_n)$ を対称式とし、$s_1, s_2, \ldots, s_n$ を $x_1, x_2, \ldots, x_n$ の基本対称式とする。

このとき、$f(x_1, x_2, \cdots, x_n)$ は $s_1, s_2, \ldots, s_n$ の多項式で書ける。

この定理を証明するために、次の定義と補題を与える。

**定義 2.7 (単項式の順序)** 次のように、$n$ 変数の単項式全体に全順序を導入する。

$d_1 = e_1, d_2 = e_2, \ldots, d_k = e_k, d_{k+1} > e_{k+1}$ を満たす $k$ が存在するとき、$x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n} > x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ と定める。

**例 2.8** 単項式 $x_1^2 x_2^1 x_3^4 x_4^7 x_5^4$ と $x_1^2 x_2^1 x_3^4 x_4^6 x_5^8$ の大小を、この定義に従って定める。

まず、$x_1$ の次数はともに 2 なので、次に $x_2$ の次数を比較する。次数はともに 1 なので、次に $x_3$ の次数を比較する。ともに次数は 4 なので、$x_4$ の次数を比較すると、前者の次数は 7 で後者の次数は 6 である。故にこの段階で決着がつき、$x_1^2 x_2^1 x_3^4 x_4^7 x_5^4 > x_1^2 x_2^1 x_3^4 x_4^6 x_5^8$ である。

**補題 2.9** 多項式 $f(x_1, x_2, \ldots, x_n)$ に出てくる単項式で順序が最大のものが $x_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$ であり、多項式 $g(x_1, x_2, \ldots, x_n)$ に出てくる単項式で順序が最大のものを $x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ とする。

このとき、多項式の積 $f(x_1, x_2, \cdots, x_n)g(x_1, x_2, \cdots, x_n)$ に出てくる単項式で順序が最大のものは $x_1^{d_1+e_1}x_2^{d_2+e_2}\cdots x_n^{d_n+e_n}$ である。

これを認めて、定理 2.6 を証明する。

今、$s_k$ $(0 \leq k \leq n)$ が $x_1, x_2, \ldots, x_n$ の $k$ 次基本対称式であるので、$s_1$ に出てくる単項式で順序が最大のものは $x_1$、$s_2$ に出てくる単項式で順序が最大のものは $x_1x_2$、$\ldots$、$s_n$ に出てくる単項式で順序が最大のものは $x_1x_2\ldots x_n$ であることに注意する。

対称式 $f(x_1, x_2, \ldots, x_n)$ に出てくる項で順序が最大のものを $ax_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$ とするとき、$d_1 \geq d_2 \geq \cdots \geq d_n$ が成り立つことを示そう。ここでは、係数付きの単項式を扱う。$d_k < d_{k+1}$ を満たす $k$ が存在したと仮定する。$f(x_1, x_2, \ldots, x_n)$ は $x_1, x_2, \ldots, x_n$ の対称式なので、$x_k$ と $x_{k+1}$ を入れ替えても不変である。故に、$f(x_1, x_2, \ldots, x_n)$ は $ax_1^{d_1}\cdots x_k^{d_{k+1}}x_{k+1}^{d_k}\cdots x_n^{d_n}$ という項を持つ。ここで、$f(x_1, x_2, \ldots, x_n)$ の項 $ax_1^{d_1}\cdots x_n^{d_n}$ とこの項の大小を比較すると、$ax_1^{d_1}\cdots x_k^{d_{k+1}}x_{k+1}^{d_k}\cdots x_n^{d_n}$ の方が $ax_1^{d_1}\cdots x_n^{d_n}$ のよりも大きい。しかしこれは $f(x_1, x_2, \ldots, x_n)$ の最大の項の取り方に反する。故に、$d_1 \geq d_2 \geq \cdots \geq d_n$ である。

ここで、多項式 $g_1(s_1, s_2, \ldots, s_n) = as_1^{d_1-d_2}s_2^{d_2-d_3}\cdots s_{n-1}^{d_{n-1}-d_n}s_n^{d_n}$ を考える。補題 2.9 より、$s_1, s_2, \ldots, s_n$ に出てくる項で順序が最大のものは、それぞれ $x_1^{d_1-d_2}$、$(x_1x_2)^{d_2-d_3}$、$\ldots$、$(x_1x_2\ldots x_n)^{d_n}$ であるので、$g_1(s_1, s_2, \cdots, s_n)$ に出てくる項で順序が最大のものは、

$$ax_1^{d_1-d_2}(x_1x_2)^{d_2-d_3}\cdots(x_1x_2\cdots x_n)^{d_n} = ax_1^{d_1}\cdots x_n^{d_n}$$

となる。

さて今、

$$f_1(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) - g_1(s_1, s_2, \cdots, s_n)$$

とすると、$f$ の $ax_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$ と $g_1$ の $ax_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$ が打ち消しあって、出てくる項で順序が最大のものの順序が下がる。この $f_1$ について $f$ に行った操作を繰り返し行う。こうして順序数を下げていくと、有限回の操作でいずれ 0 になる。つまり、

$$f(x_1, x_2, \ldots, x_n) - g_1(s_1, s_2, \ldots, s_n) - \cdots - g_m(s_1, s_2, \ldots, s_n) = 0$$

となる。従って、$f(x_1, x_2, \ldots, x_n)$ は $s_1, s_2, \ldots, s_n$ の多項式で書ける。 **証明終**

上の証明の中で使ったことではあるが、対称式の次の性質にも注意をしておこう。

**注意 2.10** $f(x_1, x_2, \ldots, x_n)$ と $g(x_1, x_2, \ldots, x_n)$ がともに $x_1, x_2, \ldots, x_n$ の対称式であるとき、$f+g$, $f-g$, $fg$ (さらに、$f$ が $g$ で割り切れるときは $\frac{f}{g}$ も) 対称式である。

# 3　差積と偶置換、奇置換

ここでは、証明に必要な道具の準備をしよう。

**定義 3.1 (差積)** $x_1, x_2, \ldots, x_n$ を $n$ 個の変数とする。

$$f(x_1, x_2, \cdots, x_n) := \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

を、$x_1, x_2, \ldots, x_n$ の差積という。

ここで、差積を特徴付ける重要な性質を述べる。

**命題 3.2** $1 \leq i < j \leq n$ とする。このとき、差積は $x_i$ と $x_j$ の入れ替えで $-1$ 倍になる。

**証明** $1 \leq i < j \leq n$ とする。
次のように、$f_1, \ldots, f_5$ を定める。

$$\begin{aligned}
f_1 &= x_i - x_j \\
f_2 &= \prod_{k<i} (x_k - x_i)(x_k - x_j) \\
f_3 &= \prod_{i<k<j} (x_i - x_k)(x_k - x_j) \\
f_4 &= \prod_{k>j} (x_i - x_k)(x_j - x_k) \\
f_5 &= \prod_{\{k,l\} \cap \{i,j\} = \emptyset,\ k<l} (x_k - x_l)
\end{aligned}$$

このとき、差積は $f = f_1 \cdots f_5$ である。
$x_i$ と $x_j$ の入れ替えで、$f_1$ は $-1$ 倍され、$f_2, \ldots, f_5$ は不変である。よって、$f$ は $x_i$ と $x_j$ の入れ替えで $-1$ 倍になる。 **証明終**

この命題によって、2 つの変数の入れ替えを行うと必ず差積は $-1$ 倍になることがわかる。従って、2 つの変数の入れ替えを偶数回行うと差積は変化せず、奇数回行うと差積は $-1$ 倍になることがわかる。
差積を不変にする入れ替えのことを偶置換と呼び、そうでないものを奇置換と呼ぶ。
次なる準備として、偶置換を表すことができる面白い道具を用意する。
今、正 12 面体の模型を一つ用意する。
正 12 面体を動かして、もとの正 12 面体に重ねる方法全体を $A$ と書く。
正 12 面体は、20 個の頂点を持ち、その頂点は 3 本の辺によって 3 つの頂点と結ばれている。ある頂点 $a$ とそのとなりの一つの頂点 $b$ に (違う) 印をつけておけば、

頂点 $a$ をどの頂点に重ねるかで 20 通りあり、頂点 $b$ をどの頂点に重ね合わせるかで 3 通りある。よって、$A$ は $20 \times 3 = 60$ 個の元からなる集合である。

一つの頂点とそれと反対の場所にある頂点を結ぶ直線を考え、その直線を軸とする $120°, 240°$ 回転は、正 12 面体を正 12 面体に重ねる。そのような回転軸の取り方は、10 通りあるので、$2 \times 10 = 20$ 通りの $A$ の元が見つかる。同じことを面で考えれば、$4 \times 6 = 24$ 通りの $A$ の元が見つかる。同じことを辺で考えれば、$1 \times 15 = 15$ 通りの $A$ の元が見つかる。まとめると、

(1) 何も動かさないもの　　1 通り
(2) 面の中心を通る軸に関する回転　$4 \times 6 = 24$ 通り
(3) 頂点を通る軸に関する回転　　$2 \times 10 = 20$ 通り
(4) 辺の中点を通る軸に関する回転　$1 \times 15 = 15$ 通り

の合計 60 個の $A$ の元が得られる。この 60 個は互いに異なる元であるので、元の個数の議論により、$A$ の各元は、上の (1), . . . , (4) のどれかであることがわかる[4]。

$A$ の元 $\xi, \eta$ に対して、その積 $\xi\eta$ を次のように定める。

**定義 3.3** $A$ の元 $\xi, \eta$ に対して、最初に正 12 面体を $\eta$ で動かし、その後 $\xi$ で動かす操作の合成を $\xi\eta$ と定義する。

上で定めた $\xi\eta$ は、明らかに $A$ の元である。

**例 3.4** 今、正 12 面体の上面と下面の中心を通る直線を回転軸として、*(*上から見て*)* 時計回りに $72°$ 回転させる操作を $\xi$ とする。ある頂点とその反対の位置にあるの頂点を通る直線を回転軸とした $120°$ 回転を $\eta$ とする。$\xi\eta$ を考えよう。

最初に $\eta$ を行えば、最初の上面と下面は、他の面に移る。次に $\xi$ を行うときは、上面と下面が移った面で定まる軸で回転させるのではない。$\xi$ を行うときは、$\eta$ を施した後の新しい上面と下面で定まる軸で *(*上から見て*)* 時計回りに $72°$ 回転させるのである。

$A$ の元は、操作と思うと考えやすい。積は、操作の合成である。

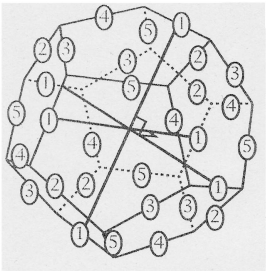
すると、結合法則、単位元の存在、逆元の存在は明らかであるので、$A$ は群になる。

次の目標は、群 $A$ が、5 次交代群 $\mathfrak{A}_5$ と同型であることを示すことである。そのために、群 $A$ から、5 次対称群 $\mathfrak{S}_5$ へ準同型写像を作りたい。

正 12 面体には辺が 30 本あり、内部には下の図のように、直交座標が 5 組隠れている。ここで、正 12 面体の内部に隠れる 5 つの直交座標に $T_i (i = 1, 2, 3, 4, 5)$ と名前をつけておく。

直交座標 $T_i$ に属する 12 面体の辺には番号 $i$ を書いておく。すると、$1, \ldots, 5$ の番号が全ての辺に重なることなく書き込まれる。

[4] $A$ の各元は $SO(3)$ の元に対応しているが、$SO(3)$ の元は必ず固有値 1 を持つ。それ故に、$A$ の各元はある軸を中心とした回転になるわけである。



さてこのように振り分けられた $1, \ldots, 5$ の番号が正 12 面体の回転 (つまり、$A$ の元) によって、どのように移るかを考える。

$A$ のある元によって直交座標 $T_i$ が直交座標 $T_j$ に移るとすれば、番号 $i$ の辺は、すべて番号 $j$ の辺があった場所へ移動する。従って $A$ の元によって、$i$ を $j$ に移すと考えれば、番号 1, 2, 3, 4, 5 の入れ替えが一つ決まることになる。

番号 $i$ の辺が番号 $j$ の辺があった場所へ移動するとき、変数 $x_1, \ldots, x_5$ で $x_i$ は $x_j$ に写ると考える。

正確に述べると、次のようになる。

**定義 3.5** $\xi \in A$ によって、直交座標 $T_1, \ldots, T_5$ がそれぞれ $T_{n_1}, \ldots, T_{n_5}$ があった場所に動いたとき、

$$\phi(\xi) = \begin{pmatrix} 1 & \cdots & 5 \\ n_1 & \cdots & n_5 \end{pmatrix}$$

によって写像 $\phi : A \to \mathfrak{S}_5$ を定める。

**補題 3.6** 写像 $\phi : A \to \mathfrak{S}_5$ は、群の準同型になる。

**証明** 今 $\xi, \eta \in A$ をとり、

$$\begin{aligned} \phi(\xi) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ m_1 & m_2 & m_3 & m_4 & m_5 \end{pmatrix}, \\ \phi(\eta) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ n_1 & n_2 & n_3 & n_4 & n_5 \end{pmatrix} \end{aligned}$$

とおく。このとき、

$$\begin{aligned} \phi(\xi)\phi(\eta) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ m_1 & m_2 & m_3 & m_4 & m_5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ n_1 & n_2 & n_3 & n_4 & n_5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ m_{n_1} & m_{n_2} & m_{n_3} & m_{n_4} & m_{n_5} \end{pmatrix} \end{aligned}$$

となる。

次に、$\phi(\xi\eta)$ を調べる。

$\eta$ によって $T_i$ が $T_{n_i}$ の場所に移り、$\xi$ によって $T_{n_i}$ が $T_{m_{n_i}}$ の場所に移るので、

$$\phi(\xi\eta) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ m_{n_1} & m_{n_2} & m_{n_3} & m_{n_4} & m_{n_5} \end{pmatrix}$$

となる。従って $\phi(\xi\eta) = \phi(\xi)\phi(\eta)$ であり、$\phi$ は群の準同型写像であることがわかった。 **証明終**

このとき次の定理が成立する。

**定理 3.7** $\xi \in A$ のとき、$\phi(\xi)$ は、差積

$$f(x_1, x_2, x_3, x_4, x_5) = \prod_{1 \le i < j \le 5} (x_i - x_j)$$

を不変にする。

また、$\phi$ は単射であり、$\phi(A) = \mathfrak{A}_5$ が成立する。*(つまり、$\phi$ によって、$A$ と $\mathfrak{A}_5$ は同型な群になる。)*

この定理の証明は、実際正 12 面体の模型を回転させてみて、入れ替えを全て書き上げ、差積が不変になることを確認すればよい。しかしここでは、群論を使ってもう少し数学的に証明してみる。

**証明** 前補題により、$\phi(A)$ は、$\mathfrak{S}_5$ の部分群であることに注意する。

$\sigma = (12345), \tau = (134)$ とすると、正 12 面体の模型を実際回転してみることで、$\sigma, \tau \in \phi(A)$ がわかる。

このとき、次が成立する。

**主張 3.8** $\mathfrak{A}_5 = <\sigma, \tau>$ が成立する。

今、上の主張が正しいと仮定しよう。すると、$\sigma, \tau \in \phi(A)$ であるので、$\mathfrak{A}_5 \subset \phi(A)$ である。しかし、$A$ の位数は 60 であり、これは $\mathfrak{A}_5$ の位数と一致している。よって、$\phi(A) = \mathfrak{A}_5$ であり、さらに $\phi$ は単射になる。すると、定理は証明されたことになる。

以下、主張の証明を行う。

$H = <\sigma, \tau>$ とおく。

$\sigma = (12345) \in \mathfrak{A}_5$ は長さ 5 の巡回置換であるので、群 $<\sigma>$ の位数は 5 である。また、$\tau = (134) \in \mathfrak{A}_5$ は長さ 3 の巡回置換であるので、群 $<\tau>$ の位数は 3 である。$<\sigma>,\quad <\tau>$ はともに $H$ の部分群なので、$H$ の位数は 3 と 5 で割り切れる。あと、$H$ が位数 4 の部分群を含むことが証明できれば、$H$ の位数は $3 \times 4 \times 5 = 60$ の倍数になり、$H = \mathfrak{A}_5$ がわかる。

$\sigma\tau\sigma^{-1} = \sigma(134)\sigma^{-1} = (\sigma(1)\sigma(3)\sigma(4)) = (245)$ である。このようにして作られる置換の共役元を次々に求めていく。

$$\begin{aligned}\sigma(245)\sigma^{-1} &= (\sigma(2)\sigma(4)\sigma(5)) = (351)\\ \sigma(351)\sigma^{-1} &= (\sigma(3)\sigma(5)\sigma(1)) = (412)\\ \sigma(412)\sigma^{-1} &= (\sigma(4)\sigma(1)\sigma(2)) = (523)\end{aligned}$$

となる。このとき、(245)(523) = (23)(45), (523)(245) = (24)(35), (23)(45)(24)(35) = (25)(34) となる。このとき、

$$\{e,\ (23)(45),\ (24)(35),\ (25)(34)\}$$

は、$H$ の位数 4 の部分群になる。

主張の証明が終わり、定理の証明が完了した。

# 4　ラグランジュの方程式

ここでは、これまで見てきた対称式論が代数方程式の解の公式の有無にどう関係するのかを考える。まずよく知られる 2 次方程式の解の公式について考えてみる。

2 次方程式 $x^2 + bx + c = 0$ の解を $\alpha_1, \alpha_2$ とすれば、

$$\alpha_i = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

で表せる。ここで対称式論を思い出そう。定理 2.3 より $b$ と $c$ は、2 次方程式の解 $\alpha_1, \alpha_2$ の基本対称式で書ける。基本対称式は対称式なので、$\alpha_1$ と $\alpha_2$ は対称式に有限回四則演算と冪根をとった式で表されている。しかし、$\alpha_1, \alpha_2$ 自身は対称式ではない。この観点から、ラグランジュ[5]は次の命題に気づいた。

**事実 4.1** “ 代数方程式に解の公式が存在する ”ならば、“ 基本対称式だけを材料にして対称でない式が作れる ”。

材料にして というのは、有限回四則演算と冪根をとった式で表されるという意味である。

$n$ 次代数方程式 $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ に対して、これが解の公式を持つならば、解を $\alpha_1, \alpha_2, \ldots, \alpha_n$ とすれば各 $\alpha_i$ が、

$\alpha_i = \alpha_1, \alpha_2, \ldots, \alpha_n$ の基本対称式に有限回の四則演算と冪根を施して得られる式

[5]ラグランジュ(Lagrange)(1736 年〜1813 年:伊)
解析学、整数論、解析力学の研究を中心に行った。解析力学では、力学と解析学を結びつけて、数学と物理の橋渡しをした。代数学の分野では、群論の萌芽として置換を研究した。1770 年には、対称式論の基本定理などを載せた『代数方程式の解についての考察』を出版した。

と書けるはずである。$\alpha_1, \alpha_2, \ldots, \alpha_n$ のうち、例えば $\alpha_i$ と $\alpha_j$ $(i \neq j$ とする) を入れ替えれば値が変わるので、$\alpha_i$ は対称式ではない。これが、上の命題の証明である。

対称式の加減乗除では対称性を崩すことはできない。2 次方程式の例で、対称式を材料にして対称でない式を作れたのは、平方根をとる操作によるのである。

実際にそれ確かめてみよう。

2 次方程式 $x^2 + bx + c = 0$ の 2 つの解を、$\alpha, \beta$ とする。このとき、

$$\alpha + \beta = -b, \quad \alpha\beta = c$$

である。ここで、$\alpha - \beta$ を考えるとこれは対称式ではないが、$(\alpha-\beta)^2$ は対称式である。

ところが、

$$(\alpha-\beta)^2 = \alpha^2 + \beta^2 - 2\alpha\beta = (\alpha + \beta)^2 - 4\alpha\beta = b^2 - 4c$$

であるので、

$$\alpha-\beta = \pm\sqrt{b^2 - 4c}$$

となり、対称でない式が基本対称式に有限回の四則演算と冪根をとった式でかけたことになる。$(\alpha-\beta)^2$ の平方根をとったときに対称性が崩れたのである。

# 5　5 次方程式の解の公式が存在しないことの証明

準備は整ったので、いよいよ 5 次方程式に解の公式が存在しないことを証明しよう。

まず証明の前に次のことに注意しておく。

5 次方程式 $x^5+a_1x^4+a_2x^3+a_3x^2+a_4x+a_5 = 0$ は、$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_5) = 0$ や $(x-\alpha_1)(x-\alpha_2)^4 = 0$ などのように、相異なる解を 2 つ以上持つ場合と、$(x-\alpha_1)^5 = 0$ と全ての解が一致する場合がある。5 次方程式に解の公式があるならば、この全ての場合において、

$$\alpha_i = s_1, s_2, \ldots, s_5 \text{ の有限回の四則演算と冪根で表された式}$$

という表現が可能だということである。

従って、5 次方程式に解の公式が存在しないことを示すには、解 $\alpha_1, \ldots, \alpha_5$ に何の因果関係もない (代数独立の場合) 場合に、上の $\alpha_i$ の式のような表現が不可能であることを示せばよい。

さて今、

$$L = \left\{ f(\alpha_1, \ldots, \alpha_5) \;\middle|\; \begin{array}{l} f \text{ は } s_1, \ldots, s_5 \text{ の有限回の四則演算と冪根をとって得られる} \\ \alpha_1, \ldots, \alpha_5 \text{ の有理式} \end{array} \right\}$$

とおく。

5 次方程式に解の公式が無いことと、$\alpha_1,\ldots,\alpha_5 \notin L$ は同値である。

それでは証明に入る。高校生に証明する場合と、(厳密な証明を与えるために) 大学の知識を使って証明する場合の 2 通りで示す。大学の知識を使った証明も、ガロア理論をまともに用いるのではなく、必要最小限の群論を使って証明する。

## 5.1 高校生に証明する場合

5 次方程式 $x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$ の相異なる 5 つの解 $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ の偶置換によって、$L$ の各元が不変になることを言えば、全ての $i$ に対して $\alpha_i \notin L$ となって、証明は終わる。

**注意 5.1** 今、置換 $\sigma \in \mathfrak{S}_5$ が、「任意の $f \in L$ に対して、$\sigma$ は $f$ を不変にする」を満たすとする。

今、差積

$$h(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = \prod_{1\leq i<j\leq 5} (\alpha_i - \alpha_j)$$

を考える。$h$ は明らかに対称式ではないが、差積の 2 乗、$H = h^2$ は対称式である。$h = \pm\sqrt{H}$ であり、また対称式の基本定理に注意すると、$h \in L$ がわかる。ここで、$h$ を不変にする置換は、偶置換のみであった。

故に $L$ のすべての元を不変にする入れ替えは、必ず偶置換である。

4 節でみたように、$L$ の元の対称性が崩れるとすれば、それは冪根をとるという操作が原因である。

よって、次の定理がいえれば不可能性が証明されたことになる。

**定理 5.2** [6] $n \in \mathbb{N}$ とする。このとき、$\alpha_1,\ldots,\alpha_5$ の有理式 $g(\alpha_1,\ldots,\alpha_5)$ に対して, $g^n$ が偶置換で不変であれば、$g$ も偶置換で不変である。

この主張を背理法により示す。つまり、

> ある自然数 $n$ と、$\alpha_1,\ldots,\alpha_5$ のある有理式 $g(\alpha_1,\ldots,\alpha_5)$ で、次を満たすものが存在すると仮定する。「$g^n$ は偶置換で不変であるが、$g$ は偶置換では不変でない。」

この条件を満たす $g$ と $n$ で、$n$ が最小になるときの $g$ と $n$ を選ぶ。

**主張 5.3** このとき、$n$ は素数である。

---

[6] 厳密に言うと、この定理から直ちに解の公式の非存在性がいえるわけではない。解の公式があると仮定したとき、解を記述するために添加する冪根が、解 $\alpha_1,\ldots,\alpha_5$ の有理式であることを保障する必要がある。

しかしその証明は大学数学の知識がないとできない。それは、補題 5.9 で示すことにする。

まず、この主張を証明する。

$n$ を合成数だと仮定する。$n = ab$ ($a, b$ は自然数で、$a \neq 1$ かつ $b \neq 1$) としよう。$g^n = (g^a)^b$ となる。

$g^a$ が偶置換で不変であれば、$g$ と $a$ が上を満たすので、$n$ の最小性に反する。

$g^a$ が偶置換で不変でなければ、$g^n$ は偶置換で不変なので、$g^a$ と $b$ が上を満たすことになり、やはり $n$ の最小性に反する。従って $n$ は素数でなければならない。

さて、$\sigma$ を任意の偶置換とし、

$$(\sigma(g))(\alpha_1, \ldots, \alpha_5) = g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(5)})$$

とおく。($\sigma$ に対応する正 12 面体の回転で、直交座標 $T_i$ が $T_j$ に移るとき、$\sigma(i) = j$ と定める。)

**主張 5.4** *$r$ を 1 の原始 $n$ 乗根とすると、$\sigma(g) = r^i g$ と書ける。*

この主張を証明する。

$$((\sigma(g))(\alpha_1, \ldots, \alpha_5))^n = (g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(5)}))^n$$

であり、一方 $g^n$ が偶置換で不変であるので、

$$(g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(5)}))^n = (g(\alpha_1, \ldots, \alpha_5))^n$$

である。よって $(\sigma(g))^n = g^n$ であり、$\sigma(g)$ は $z^n = g^n$ の解であることがわかり、$\sigma(g) = r^i g$ となる。

次を証明する。

**主張 5.5** *(1) $g$ を不変にする偶置換は $\dfrac{60}{n}$ 個存在する。*

*(2) $H$ を $g$ を不変にする偶置換全体とするとき、*

- *(2-1) $H$ は正 12 面体の面の中心を通る軸に関する回転を全て含むか、1 つも含まないかのどちらかである。*
- *(2-2) $H$ は正 12 面体の頂点を通る軸に関する回転を全て含むか、1 つも含まないかのどちらかである。*
- *(2-3) $H$ は正 12 面体の辺の中点を通る軸に関する回転を全て含むか、1 つも含まないかのどちらかである。*
- *(2-4) $H$ は何も動かさない回転を含む。*

(1) を証明する。

今、各 $i = 0, 1, 2, \ldots, n-1$ に対して、

$$B_i \stackrel{\text{def}}{=} \{\sigma \in \mathfrak{A}_5 \mid \sigma(g) = r^i g\}$$

としよう。このとき、任意の $i$ に対して $B_i$ は空でないことを示そう。

最初に $B_1, B_2, \ldots, B_{n-1}$ の中に少なくとも一つは空でないものがあることを示す。$1 \leq i \leq n-1$ を満たす全ての $i$ に対し、$B_i = \emptyset$ であると仮定すると、$B_0$ が偶置換全体 $\mathfrak{A}_5$ となる。このとき $g$ は偶置換で不変となるので $g$ の取り方に反する。故に $B_1, B_2, \ldots, B_{n-1}$ には少なくとも 1 つ空でないものが存在する。さてその集合を $B_j$ としよう。

$B_j$ の元 $\sigma$ を一つとる。$\sigma(g) = r^j g$ となることに注意する。このとき、

$$\sigma(g) = r^j g \Rightarrow \sigma^2(g) = r^{2j} g \Rightarrow \sigma^3(g) = r^{3j} g \Rightarrow \cdots \Rightarrow \sigma^{n-1}(g) = r^{(n-1)j} g$$

となる。ここで $n$ が素数であることに注意すると $g.c.d(j, n) = 1$ なので、$aj + bn = 1$ をみたす整数 $a, b$ がある。このとき、任意の整数 $q$ に対して、$(a+qn)j + (b-qj)n = 1$ を満たすので、必要なら $a$ を $a + qn$(ただし、$q$ は大きな自然数にとる) と取り替えることにより、$a$ は自然数であると仮定してよい。

$\sigma^a(g) = r^{aj} g$ であるので、$aj + bn = 1$ より $aj \equiv 1 \pmod{n}$ なので、$\sigma^a(g) = rg$ である。このとき、$\sigma^{2a}(g) = r^2 g, \sigma^{3a}(g) = r^3 g, \ldots, \sigma^{(n-1)a}(g) = r^{n-1} g$ となる。

従って、$\sigma^a \in B_1, \sigma^{2a} \in B_2, \ldots, \sigma^{(n-1)a} \in B_{n-1}$ となって、$B_1, B_2, \ldots, B_{n-1}$ はいずれも空でない。勿論 $B_0$ も空でないから、全ての $B_i$ は空でない集合である。

次に各 $i = 1, 2, \ldots, n-1$ に対して、$\sharp B_0 = \sharp B_i$ となることを示す。

$i$ を一つ任意に固定し、$\tau \in B_i$ をとる。今、写像 $\Phi : B_0 \to B_i$ を $\Phi(\sigma) = \tau\sigma$ で定め ($\sigma \in B_0$ のとき、$\tau\sigma \in B_i$ であることは容易にチェックできる)、写像 $\Psi : B_i \to B_0$ を $\Psi(\rho) = \tau^{-1}\rho$ で定める ($\rho \in B_i$ のとき、$\tau^{-1}\rho \in B_0$ であることは容易にチェックできる)。

このとき、$\Phi$ と $\Psi$ は互いに逆射となっている[7]。

従って、各 $i = 1, 2, \ldots, n-1$ に対して、$\sharp B_0 = \sharp B_i$ となることが分かった。こうして、$\sharp B_0 (= \sharp H) = \sharp B_1 = \sharp B_2 = \cdots = \sharp B_{n-1}$ となり、$\sharp H = \dfrac{60}{n}$ が成り立つ。 **証明終**

次に、(2) を証明する。

(2 − 4) は明らかである。(2 − 1) が証明できれば、(2 − 2), (2 − 3) の証明も同じようにしてできる。(2 − 1) のみを示そう。

まず次のことを示す。

> “ 面の軸を通る (非自明な) 回転の中で、一つでも $g$ を不変にするものがあれば、その軸に関する全ての回転で $g$ は不変になる。”(★)

[7]大学の数学の言葉を使えば、次のように簡単にチェックできる。$(\Psi\Phi)(\sigma) = \Psi(\Phi(\sigma)) = \Psi(\tau\sigma) = \tau^{-1}(\tau\sigma) = \sigma$ となる。故に、$\Psi\Phi = id_{B_0}$ となる。また、$(\Phi\Psi)(\rho) = \Phi(\Psi(\rho)) = \Phi(\tau^{-1}\rho) = \tau(\tau^{-1}\rho) = \rho$ となる。故に、$\Phi\Psi = id_{B_i}$ となる。よって、$\Phi$ と $\Psi$ は互いに逆射である。

しかし、高校生には例えば次のような表面的な証明しかできない。$\tau$ を $g$ を $r^i g$ へ移す回転として 1 つ固定する。$\sigma \in B_0$ に対して、$g$ を $r^i g$ に移す回転 $\tau\sigma$ が丁度 1 つ決まる。また、$\rho \in B_i$ に対して、$g$ を $g$ に移す回転 $\tau^{-1}\rho$ が丁度 1 つ決まる。よって、$B_0$ の元と $B_i$ の元が 1 本 1 本線で結べるので、$\sharp B_0 = \sharp B_i$ がわかる。

まず72°の回転が $g$ を不変にする場合を考えよう。その回転を $A$ とすれば、144°回転は $A^2$ で表され、-144°回転は $A^3$ で表され、-72°回転は $A^4$ で表される。$g$ を不変にする回転を何度やっても、やはり $g$ を不変にするから、$A^2$、$A^3$、$A^4$ も $g$ を不変にする。

次に、144°の回転が $g$ を不変にする場合を考えよう。その回転を $B$ とすれば、-72°回転は $B^2$ で表され、72°回転は $B^3$ で表され、-144°回転は $B^4$ で表される。$B$ が $g$ を不変にすれば、やはり $B^2$、$B^3$、$B^4$ も $g$ を不変にする。

-72°や-144°の回転が $g$ を不変にする場合も同じことがいえる。以上より $(\star)$ がいえた。

次に、面の中心を通る回転軸 $L$ と $M$ があり、$L$ での回転で $g$ が不変であるとき、$M$ での回転でも $g$ が不変になることを示す。

そこで $L$ の面を $M$ の面に移す回転の1つを $B$ とし、$g$ を不変にする $L$ に関する回転の一つを $A$ とする。$(\star)$ が示されているので、$M$ の回転で $g$ を不変にするものを1つみつければよい。

今 $B$ の逆回転を $B^{-1}$ とし、回転 $C : BAB^{-1}$ を考える。この回転は軸 $M$ に関する回転である。実際、軸 $M$ 上に点 $P$ をとるとき、$P$ は $B^{-1}$ で $L$ へ移動し、$A$ では動かず $B$ で再び $M$ に戻る。すなわち点 $P$ は不動であり、回転 $C$ は軸 $M$ に関する回転である。

$C$ によって $g$ は再び $g$ へと移るのは明らかである[8]。こうして、軸 $M$ に関する回転で $g$ を不変にするものがみつかった。

以上より、$(2-1)$ が示された。 **証明終**

この事実の下で $H$ の元数が絞られる。$H$ が (2-1)〜(2-3) の各場合において、軸の回転を全て含むときは○、1つも含まないときを×で表すと次の (i) から (viii) の8通りが考えられる。

| | $(2-1)$ | $(2-2)$ | $(2-3)$ | $(2-4)$ |
|---|---|---|---|---|
| $(i)$ | ○ | ○ | ○ | ○ |
| $(ii)$ | ○ | ○ | × | ○ |
| $(iii)$ | ○ | × | ○ | ○ |
| $(iv)$ | × | ○ | ○ | ○ |
| $(v)$ | ○ | × | × | ○ |
| $(vi)$ | × | ○ | × | ○ |
| $(vii)$ | × | × | ○ | ○ |
| $(viii)$ | × | × | × | ○ |

[8] $i$ を、$g$ が $B^{-1}$ で $r^i g$ になるようにとる。回転 $A$ は $g$ を不変にするので $r^i g$ も不変にする。そして、$r^i g$ は $B$ によって $g$ に戻る。故に、$g$ は $C$ で不変である。

$$g \xrightarrow{B^{-1}} r^i g \xrightarrow{A} r^i g \xrightarrow{B} g$$

この表により (i) から (viii) の各場合において $H$ の位数は、60, 45, 40, 36, 25, 21, 16, 1 のいずれかであることが分かる。事実 (1) により $H$ の位数は 60 の約数であるから、考えられるのは 1 か 60 である。$\sharp H$=1 ならば、$n$=60 であるが、$n$ は素数であったのでこれは矛盾。また、$\sharp H = 60$ ならば、$n = 1$ であるのでやはり $n$ が素数であることに反する。よって主張が正しいことが示された。

こうして、定理 5.2 が示されたので 5 次方程式は解の公式を持たないことが証明された。 **証明終**

## 5.2 大学の知識を使って証明する場合

さて大学生に証明するための準備をしよう。

$\mathbb{C}$ 上代数独立な元 $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ を解に持つ 5 次方程式 $x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$ について考える。

$$\mathbb{C}[\alpha_1, \ldots, \alpha_5] = \left\{ h(\alpha_1, \ldots, \alpha_5) \;\middle|\; \begin{array}{l} h \in \mathbb{C}[X_1, \ldots, X_5] \\ \mathbb{C}[X_1, \ldots, X_5] \text{ は 5 変数多項式環} \end{array} \right\}$$

とおくと、これは $\mathbb{C}$ 上 5 変数の多項式環と同型である。$\mathbb{C}[\alpha_1, \ldots, \alpha_5]$ は整域が故、有理関数体

$$\mathbb{C}(\alpha_1, \ldots, \alpha_5) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_5)}{g(\alpha_1, \ldots, \alpha_5)} \;\middle|\; \begin{array}{l} f \in \mathbb{C}[X_1, \ldots, X_5] \\ g \in \mathbb{C}[X_1, \ldots, X_5]\text{-}\{0\} \\ g(\alpha_1, \ldots, \alpha_5) \neq 0 \end{array} \right\}$$

が考えられる。次の定理に注意しよう。

**定理 5.6** $\sigma \in \mathfrak{S}_5$ に対して、

$$\begin{array}{rcl} \sigma : \mathbb{C}(\alpha_1, \ldots, \alpha_5) & \to & \mathbb{C}(\alpha_1, \ldots, \alpha_5) \\ \dfrac{f(\alpha_1, \ldots, \alpha_5)}{g(\alpha_1, \ldots, \alpha_5)} & \mapsto & \dfrac{f(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(5)})}{g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(5)})} \end{array}$$

という体上の準同型写像が定まる。

**証明** 今 $\sigma \in \mathfrak{S}_5$ に対して、$f(\alpha_1, \ldots, \alpha_5) \mapsto f(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(5)})$ によって引き起こされる環の単射準同型写像 $\sigma : \mathbb{C}[\alpha_1, \ldots, \alpha_5] \to \mathbb{C}[\alpha_1, \ldots, \alpha_5]$ が決まる。

ここで、$f(\alpha_1, \ldots, \alpha_5) \mapsto \frac{f(\alpha_1, \ldots, \alpha_5)}{1}$ で定まる単射準同型写像 $\eta : \mathbb{C}[\alpha_1, \ldots, \alpha_5] \to \mathbb{C}(\alpha_1, \ldots, \alpha_5)$ について考える。$\eta$ が単射なので、任意の $g(\alpha_1, \ldots, \alpha_5) \in \mathbb{C}[\alpha_1, \ldots, \alpha_5]$ に対して、$(\eta(\sigma))(g(\alpha_1, \ldots, \alpha_5)) \neq 0$ である。よって、$(\eta(\sigma))(g(\alpha_1, \ldots, \alpha_5)) \in U(\mathbb{C}(\alpha_1, \ldots, \alpha_5))$ であることがわかる。

従って、環の局所化の性質により環の準同型写像 $h : \mathbb{C}(\alpha_1, \ldots, \alpha_5) \to \mathbb{C}(\alpha_1, \ldots, \alpha_5)$ で、$\eta(\sigma) = hi$ を満たすものがある。ただし、$i : \mathbb{C}[\alpha_1, \ldots, \alpha_5] \to \mathbb{C}(\alpha_1, \ldots, \alpha_5)$

は、包含写像とする。このとき、$\frac{f(\alpha_1,\ldots,\alpha_5)}{g(\alpha_1,\ldots,\alpha_5)} \in \mathbb{C}(\alpha_1,\ldots,\alpha_5)$ に対して、$h(\frac{f(\alpha_1,\ldots,\alpha_5)}{g(\alpha_1,\ldots,\alpha_5)}) = \frac{f(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(5)})}{g(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(5)})}$ となる。

こうして $h$ を改めて $\sigma$ と書いて、体上の準同型写像 $\sigma : \mathbb{C}(\alpha_1,\ldots,\alpha_5) \to \mathbb{C}(\alpha_1,\ldots,\alpha_5)$ が定まった。 **証明終**

**系 5.7** $\mathfrak{S}_5 \curvearrowright \mathbb{C}(\alpha_1,\ldots,\alpha_5)$ となる。

つまり、$\mu : \mathfrak{S}_5 \times \mathbb{C}(\alpha_1,\ldots,\alpha_5) \to \mathbb{C}(\alpha_1,\ldots,\alpha_5)$ を、$(\sigma, \frac{f(\alpha_1,\ldots,\alpha_5)}{g(\alpha_1,\ldots,\alpha_5)}) \mapsto \frac{f(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(5)})}{g(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(5)})}$ という写像とすれば、$\mu$ は群の作用の公理を満たす。

さらに、ガロア拡大 $\mathbb{C}(\alpha_1,\ldots,\alpha_5)/\mathbb{C}(s_1,\ldots,s_5)$ のガロア群は、$\mathfrak{S}_5$ である。

ここで、

$$L = \left\{ f(\alpha_1,\ldots,\alpha_5) \;\middle|\; \begin{array}{l} f \text{ は } s_1,\ldots, s_5 \text{ の有限回の四則演算と冪根をとって得られる} \\ \alpha_1,\ldots, \alpha_5 \text{ の有理式} \end{array} \right\}$$

を思い出そう。明らかに $L$ は、$\mathbb{C}(s_1,\ldots,s_5)$ 上の正規拡大であるから、$\mathfrak{S}_5 \curvearrowright L$ となる。

さて今、$L$ に対して、

$$I(L) = \left\{ \sigma \in \mathfrak{S}_5 \;\middle|\; \forall f \in L, \sigma(f) = f \right\}$$

とおく。$I(L)$ は $\mathfrak{S}_5$ の部分群である。

5 次方程式 $x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$ が解の公式を持つことと、$\mathbb{C}(\alpha_1,\ldots,\alpha_5) = L$ は同値である。また、ガロアの基本定理により、このことは、$I(L) = \{e\}$ と同値である。

従って、5 次方程式 $x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$ に解の公式が存在しないことを示すには、$I(L) \neq \{e\}$ を示せばよい。$L$ は差積を含んでいる。差積を不変にするのは、偶置換のみであるので、$I(L) \subset \mathfrak{A}_5$ がわかる。そこで $I(L) \neq \{e\}$ を示すために、$\mathfrak{A}_5 = I(L)$ を示そう。

まず、体論に関する準備が必要である。

**定義 5.8** $E/F$ を体拡大とする。適当な正整数 $n$ に対して、$\alpha^n \in F$ となる $\alpha \in E$ を使って $E = F(\alpha)$ と表せるとき、$E/F$ は $n$ 型純拡大という。体の拡大の列

$$F = R_0 \subset R_1 \subset \cdots \subset R_s$$

は、おのおのの $R_i/R_{i-1}$ が純拡大のとき、冪根搭という。このとき、$R_s/F$ を冪根拡大と呼ぶ。

$L$ の定義により、$L$ を含む $\mathbb{C}(s_1,\ldots,s_5)$ の有限次冪根拡大 $M$ が存在する。$K = \mathbb{C}(s_1,\ldots,s_5), L = F, M = E$ として、次の補題を使えば、$L$ は $\mathbb{C}(s_1,\ldots,s_5)$ の冪根拡大であることがわかる。

**補題 5.9** $\mathbb{C} \subset K \subset F \subset E$ を体の拡大とする。$E/K$ が有限次冪根拡大で、$F/K$ がガロア拡大ならば、$F/K$ は冪根拡大となる。

**証明** 拡大次数 $[F : K]$ に関する帰納法で証明する。$F = K$ のときは自明に正しいので、$[F : K] \geq 2$ としよう。

仮定より、冪根塔

$$K = K_0 \subset K_1 \subset \cdots \subset K_l = E$$

が存在する。ここで、それぞれの $i$ に対して、$K_i/K_{i-1}$ は $n_i$ 型純拡大とする。ここで、全ての $i$ に対して、$n_i$ は素数としてよい。

このとき、

$$K = K_0 \cap F \subset K_1 \cap F \subset \cdots \subset K_l \cap F = F$$

である。ここで、

$$K = K_{i-1} \cap F \neq K_i \cap F$$

と仮定する。

まず、$K_i \cap F/K$ はガロア拡大であることを示す。$a \in K_i \cap F$ の $K_{i-1}$ 上のモニック最小多項式を $f(x)$ としよう。$b$ が $f(x)$ の根であれば、$a$ と $b$ は $K$ 上共役である。$a \in F$ であるので、$b \in F$ である。($F$ は $K$ 上ガロア拡大であることに注意。) よって、$f(x)$ の係数は $F$ に入る。結局、$f(x)$ の係数は $K = K_{i-1} \cap F$ に入り、$f(x)$ は $a$ の $K$ 上の最小多項式になる。よって、$a$ の $K$ 上の共役は、$f(x)$ の根になり、従って $K_i \cap F$ の元である。よって、$K_i \cap F/K$ はガロア拡大である。

ガロア群の作用を自然に制限することにより、

$$\mathrm{Gal}(K_i/K_{i-1}) \xrightarrow{\phi} \mathrm{Gal}(K_i \cap F/K_{i-1} \cap F)$$

という群準同型が得られる。$\phi$ の像を $G$ とする。このとき、

$$(K_i \cap F)^G \subset K_i^G \cap (K_i \cap F) \subset K_{i-1} \cap F$$

である。ガロアの基本定理により、$G = \mathrm{Gal}(K_i \cap F/K_{i-1} \cap F)$ になる。今、$\mathrm{Gal}(K_i/K_{i-1})$ の位数は素数 $n_i$ であるので、$G$ の位数も $n_i$ となる。

このとき、拡大 $K_i \cap F/K$ は、素数次のガロア拡大であるので、純拡大であることがわかる。

$$\mathbb{C} \subset K_i \cap F \subset F \subset E$$

に対して帰納法の仮定が適用でき、$F/K$ は冪根拡大であることがわかった。

**証明終**

前補題により、$L$ は $\mathbb{C}(s_1, \ldots, s_5)$ の冪根拡大であることがわかった。冪根塔

$$\mathbb{C}(s_1, \ldots, s_5) = K_0 \subset K_1 \subset \cdots \subset K_l = L$$

をとる。ここで、$K_i/K_{i-1}$ は $n_i$ 型の純拡大としよう。各 $n_i$ は素数であるとしてよい。また、$K_1$ は、$K_0$ に根の差積を添加した体であると仮定してよい。

ここで、次を証明する。

**主張 5.10** $i \geq 2$ に対して、$I(K_{i-1}) = \mathfrak{A}_5$ であれば、$I(K_i) = \mathfrak{A}_5$ である。

これがいえれば、$I(L) = \mathfrak{A}_5$ がわかり、証明が完了する。

上の主張を証明する[9]。

$i \geq 2$ とし、$K_i = K_{i-1}(g)$ とする。ただし、$g^n \in K_{i-1}$ とする。今、次のような写像を定義する。

$$\begin{aligned} \Phi : \mathfrak{A}_5 &\to \mathbb{C}^\times \\ \sigma &\mapsto \sigma(g)g^{-1} \end{aligned}$$

このとき $\Phi$ は群の準同型写像になる[10]。$Ker(\Phi) \triangleleft \mathfrak{A}_5$ であり $\mathfrak{A}_5$ は単純群なので、$Ker(\Phi) = \{e\}$ または $Ker(\Phi) = \mathfrak{A}_5$ となる。ここで $Ker(\Phi) = \{e\}$ と仮定すると、群の準同型定理より、$\mathfrak{A}_5/Ker(\Phi) \cong \mathfrak{A}_5$ となる。しかし、$\mathfrak{A}_5/Ker(\Phi)$ はアーベル群で $\mathfrak{A}_5$ はアーベル群でないので矛盾する。従って、$Ker(\Phi) = \mathfrak{A}_5$ がわかる。
このとき、任意の $\mathfrak{A}_5$ の元 $\sigma$ に対して、$\Phi(\sigma(g)) = \sigma(g)g^{-1} = 1$ となるので、$\sigma(g) = g$ となる。こうして、$I(K_i) = \mathfrak{A}_5$ がわかった。

# 6　付録　4 次以下の代数方程式の解の公式について

ここでは、4 次以下の代数方程式の解の公式について考えてみる。

1 次方程式 $ax + b = 0 (a \neq 0)$ の解の公式は、$x = -\dfrac{b}{a}$ である。

2 次方程式 $ax^2 + bx + c = 0 (a \neq 0)$ の解の公式は、中学校で学んだように、

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

である。3 次方程式の解の公式はイタリアの数学者タルターリャ(Tartaglia) と、医師カルダノ (Cardano) によって発見され応用化された。

それではまず、3 次方程式 $x^3 + px + q = 0 (p, q \in \mathbb{C})$ の解の公式をタルターリャが発見した方法で求めてみよう。

$p = 0$ のときは明らかであるので、$p \neq 0$ であると仮定しよう。

---

[9] この証明は後藤四郎教授に指導をしていただきました。

[10] $\sigma_1, \sigma_2 \in \mathfrak{A}_5$ に対して、$\Phi(\sigma_1\sigma_2) = \Phi(\sigma_1)\Phi(\sigma_2)$ を示す。
今、$\sigma_1(g) = r^j g, \sigma_2(g) = r^k g$ とかくことにする。このとき、

$$\Phi(\sigma_1\sigma_2) = (\sigma_1\sigma_2)(g)g^{-1} = \sigma_1(\sigma_2(g))g^{-1} = \sigma_1(r^k g)g^{-1} = r^j(r^k g)g^{-1} = r^{j+k}$$

となる。一方で、

$$\Phi(\sigma_1)\Phi(\sigma_2) = (\sigma_1(g)g^{-1})(\sigma_2(g)g^{-1}) = (r^j g g^{-1})(r^k g g^{-1}) = r^j r^k = r^{j+k}$$

となる。故に、$\Phi(\sigma_1\sigma_2) = \Phi(\sigma_1)\Phi(\sigma_2)$ となり、$\Phi$ は群の準同型写像である。

高校生のときに学んだ $x^3+y^3+z^3-3xyz$ の因数分解

$$x^3+y^3+z^3-3xyz=(x+y+z)(x^2+y^2+z^2-xy-yz-xz)$$

が、ここで重要な役割を果たす。タルターリャの発想は、$x^3+px+q=x^3+y^3+z^3-3xyz$ となるように $y$ と $z$ を $p$ と $q$ を使って表せれば、$x^3+y^3+z^3-3xyz$ が因数分解できることから $x^3+px+q=0$ の解の公式が得られる! というものであった。

$$x^3+px+q=x^3+y^3+z^3-3xyz \Longleftrightarrow \begin{cases} p=-3yz & \cdots \quad (1) \\ q=y^3+z^3 & \cdots \quad (2) \end{cases}$$

となる。$p=-3yz$ ならば $p^3=-27y^3z^3$ であるので、$z^3=-\dfrac{p^3}{27y^3}$ となる。これを (2) に代入して整理すると、

$$y^6-qy^3-\frac{p^3}{27}=0$$

となる。そして $y^3$ について解くと、2 次方程式の解の公式によって、

$$y^3=\frac{q\pm\sqrt{q^2+\frac{4}{27}p^3}}{2}$$

となる。今、

$$\alpha^3=\frac{q+\sqrt{q^2+\frac{4}{27}p^3}}{2}$$

を満たすとする。ここで、

$$y=\alpha,\ \ z=-\frac{p}{3\alpha}$$

とおくと、$y$ と $z$ は、上の (1), (2) を満たす。よって、$-y-z$ は、$x^3+px+q=0$ の解である。残りの解は、二次方程式を解いて得られる。

今みた 3 次方程式は、2 次の項がなかった。2 次の項を含む一般の 3 次方程式 $x^3+ax^2+bx+c=0$ を扱う場合は、次のカルダノ変換を用いる。

**主張 6.1** *(カルダノ変換)*[11] $f(x)=x^3+ax^2+bx+c\in\mathbb{C}[x]$ とする。$x$ を $X-\dfrac{a}{3}$ に置き換えると、2 次の項が消去された多項式:$F(X)=X^3+(b-\frac{1}{3}a^2)X+(\frac{2a^3}{27}-\frac{ab}{3}+c)$ が得られる。

$x^3+ax^2+bx+c=0$ をカルダノ変換して得られる多項式 $F(X)\in\mathbb{C}$ についての方程式 $F(X)=0$ はタルターリャの方法で解ける。今、$F(X)=0$ の一つの解を $u$ とする。$x=u-\dfrac{a}{3}$ と置いて $f(x)$ に代入すると、$f(u-\frac{a}{3})=0$ となる。つまり $x=u-\dfrac{a}{3}$ は $x^3+ax^2+bx+c=0$ の解の一つである。

[11] 一般に、考える多項式の最高次の次数が $n$ の場合は、カルダノ変換によって $n-1$ 次の項を消去できる。

最後に、4次方程式 $x^4+ax^3+bx^2+cx+d=0$ の解の公式について考えよう。4次方程式は3次方程式に帰着できる。今 $f(x)=x^4+ax^3+bx^2+cx+d$ として、$x=X-\frac{a}{4}$ を $f(x)$ に代入してカルダノ変換しよう。変換によって、$F(X)=X^4+pX^2+qX+r$ という形の多項式が得られるはずである。さて今、$k,m,l$ を定数として、

$$X^4+pX^2+qX+r=(X^2+kX+l)(X^2-kX+m)$$

となるように、$k,m,l$ を既知定数 $p,q,r$ を用いて表す。

$$(X^2+kX+l)(X^2-kX-m)=X^4+(m-k^2+l)X^2+(m-l)kX+lm$$

となる。従って、

$$X^4+pX^2+qX+r=(X^2+kX+l)(X^2-kX+m)\Longleftrightarrow\begin{cases}p=m-k^2+l & \cdots\quad(3)\\ q=(m-l)k & \cdots\quad(4)\\ r=lm & \cdots\quad(5)\end{cases}$$

となる。(3) と (4) を連立すると、

$$\begin{cases}2m=k^2+\frac{q}{k}+p & \cdots\quad(6)\\ 2l=k^2-\frac{q}{k}+p & \cdots\quad(7)\end{cases}$$

を得て、(6) と (7) より $4ml=(p+k^2)^2-\frac{q^2}{k^2}$ を得る。(5) をこの方程式に代入すれば、

$$4ml=(p+k^2)^2-\frac{q^2}{k^2}\Longleftrightarrow k^6+2pk^4+(p^2-4r)k^2-q^2=0\cdots(8)$$

となる。ここで $t=k^2$ と置くと、$(8)\Longleftrightarrow t^3+2pt^2+(p^2-4r)t-q^2=0$ となり、この3次方程式をカルダノ変換してタルーリャの方法で $k$ を求めることができる。(6) と (7) に注意すれば、

$$X^4+pX^2+qX+r=\{X^2+kX+\frac{1}{2}(k^2-\frac{q}{k}+p)\}\{X^2+kX+\frac{1}{2}(k^2+\frac{q}{k}+p)\}$$

となる。

あとは、二次方程式を解の公式を使って解けばよい。