5次方程式の解の公式に関するアーベルの定理

§ プロローグ/代数方程式の解と係数の関係から対称式の理論へ

2次方程式 $x^2-ax+b=0$ の解 α,β と係数 a,b の関係は $a=\alpha+\beta$　$b=\alpha\beta$

a,b 式の中で α と β を交換しても同じになる。このような式を α,β の対称式という。

代数方程式の解の公式の理解のためには、対称式を理解する必要がある。

§ 対称式の理論

群の定義の知識を前提とする。有限集合 $\Sigma_n=\{1,2,\cdots,n\}$ から Σ_n への全単射を n 次の**置換**という。

置換 σ の k と $\sigma(k)$ $(k=1,2,\cdots,n)$ の対応表を次のように書く。 $\sigma(k)=k$ の時は表から省略できる。

$$\sigma=\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$$

[例] $\Sigma_6=\{1,2,3,4,5,6\}$　$\sigma(1)=1,\sigma(2)=3,\sigma(3)=6,\sigma(4)=2,\sigma(5)=5,\sigma(6)=4$ の対応表は

$$\sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 2 & 5 & 4 \end{pmatrix}=\begin{pmatrix} 2 & 3 & 4 & 6 \\ 3 & 6 & 2 & 4 \end{pmatrix}$$

置換 $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ を**単位元**といい、 $\boldsymbol{e}$ と書く。

置換 $\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$ を σ の**逆置換**といい、 σ^{-1} と書く。

置換 σ,τ の**積**を次のように定義する。 $\sigma\cdot\tau$ $=$ $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}$

σ の n 回の積を $\sigma\cdot\sigma\cdots\sigma=\sigma^n$ と書く。

n 次の置換すべての集合 S_n は置換の積により群となり、**対称群**という。その部分群を**置換群**という。

置換群 G の元が G の部分集合 A の元の積で表せるとき、 A は G を**生成**するという。

置換 $\begin{pmatrix} i & j \\ j & i \end{pmatrix}$ （ $i<j$ ）を**互換**といい、 $\boldsymbol{(i,j)}$ と書く。 $(i,j)^2=e$ である。

置換 $\begin{pmatrix} i_1 & i_2 & \cdots & i_{k-1} & i_k \\ i_2 & i_3 & \cdots & i_k & i_1 \end{pmatrix}$ を $\boldsymbol{k}$ **サイクル**といい、 $\boldsymbol{(i_1 i_2\cdots i_k)}$ と書く。

[補題] 互換の集合は S_n を生成する。 系として $(1,k)$ $(k=2,3,\cdots,n)$ は S_n を生成する。

[証明] $S_2=\{(1,2)^2,(1,2)\}$ より $n=2$ で正しい。 $n=k$ を仮定。 $\sigma\in S_{k+1}$ → $\tau=(k+1,\sigma(k+1))\cdot\sigma$ は $\tau(k+1)=k+1$ だから $\tau\in S_k$ なので互換の積になり、 $\sigma=(k+1,\sigma(k+1))\tau$ も互換の積で表せる。

さらに $(i,j)=(1,j)(1,i)(1,j)$ だから補題の系も証明された。■

[**補題**] S_n は互換 $(1,2)$ と n サイクル $(12\cdots n)$ とによって生成される。

[証明] サイクルの性質 $(a_1,a_2,\cdots,a_k,\cdots,a_s)=(a_1,a_2,\cdots,a_k)(a_k,a_{k+1},\cdots,a_s)$ より

$\sigma=(1,2)(1,2,\cdots,n)=(1,2)(1,2)(2,3,\cdots,n)$ $=$ $(2,3,\cdots n)$ よって $1\le k\le n-2$ に対して $\begin{matrix}\sigma^k(1)=1\\ \sigma^k(2)=2+k\end{matrix}$

$\sigma^k(1,2)\sigma^{-k}(1)=\sigma^k(1,2)(1)=\sigma^k(2)=2+k$

$\sigma^k(1,2)\sigma^{-k}(2+k)=\sigma^k(1,2)(2)=\sigma^k(1)=1$

$m\neq 1,2+k$ の時 $\sigma^{-k}(m)\neq 1,2$ → $\sigma^k(1,2)\sigma^{-k}(m)=\sigma^k\sigma^{-k}(m)=m$

以上から $\sigma^k(1,2)\sigma^{-k}=(1,2+k)$ ゆえに $(1,j)$ $(j=3,4,\cdots,n)$ を表せるので前補題より証明された。■

[**補題**] 写像 $c:\sigma\in S_n\to c(\sigma)\in C$ （ C は複素数の集合)が

$c(e)\neq 0$ かつ $c(\tau\cdot\sigma)=c(\tau)c(\sigma)$ を満たすとき、準同型写像という。

この時、すべての互換 τ について $c(\tau)^2=1$ かつ $c(\tau)=c((1,2))$ が成立する。

[証明] $c(e)=c(e\cdot e)=c(e)^2$ かつ $c(e)\neq 0$ より $c(e)=1$

互換 τ について $\tau^2=e$ なので $c(\tau)^2=c(\tau^2)=c(e)=1$

$n\ge 3$　$j\ge 3$ の時 $(1,j)=(2,j)(1,2)(2,j)$ なので

$c((1,j))=c((2,j))c((1,2))c((2,j))=c((1,2))c((2,j))^2=c((1,2))$ よって前補題から証明された。■

●置換の作用

関数を多項式またはその分数式に限定する。多変数多項式は既約多項式の積に(定数倍の差を除いて)一意に分解できる。多項式 f と g に共通の因子が(定数の他は)ない時 f と g を**互いに素**という。

n 変数関数 $f(x_1,x_2,\cdots,x_n)$ について、置換 σ の**作用** $\sigma\cdot f$ を次のように定義する。

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

・置換群の単位元 e の作用について $e\cdot f=f$

・四則演算+, −, ×, ÷を ○で表すと $\sigma(f\bigcirc g)=(\sigma f)\bigcirc(\sigma g)$ (置換は準同型写像)→ $\sigma f^n=(\sigma f)^n$

[証明] $\sigma(f(x_1,x_2,\cdots,x_n)\bigcirc g(x_1,x_2,\cdots,x_n))$ = $(f(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)})\bigcirc g(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)}))$

= $(\sigma f(x_1,x_2,\cdots,x_n))\bigcirc(\sigma g(x_1,x_2,\cdots,x_n))$ ■

[定理:置換の積と作用の関係式]

置換 σ,τ と関数 f について $\tau\cdot(\sigma\cdot f)=(\tau\cdot\sigma)\cdot f$

[証明] 関数 $g=\sigma\cdot f$ に置換 τ を作用させると

$(\tau\cdot g)(x_1,x_2,\cdots,x_n)=g(x_{\tau(1)},x_{\tau(2)},\cdots,x_{\tau(n)})$

そこで $y_1=x_{\tau(1)},y_2=x_{\tau(2)},\cdots,y_n=x_{\tau(n)}$ とおいて

$g(x_{\tau(1)},x_{\tau(2)},\cdots,x_{\tau(n)})=g(y_1,y_2,\cdots,y_n)$ = $(\sigma\cdot f)(y_1,y_2,\cdots,y_n)=f(y_{\sigma(1)},y_{\sigma(2)},\cdots,y_{\sigma(n)})$ ($g=\sigma\cdot f$ より)

$y_j=x_{\pi(j)}$ に $j=\sigma(q)$, $(q=1,2,\cdots,n)$ を代入すると $y_{\sigma(q)}=x_{\pi(\sigma(q))}$ より

$f(y_{\sigma(1)},y_{\sigma(2)},\cdots,y_{\sigma(n)})$ = $f(x_{\tau(\sigma(1))},x_{\tau(\sigma(2))},\cdots,x_{\tau(\sigma(n))})$ = $f(x_{(\tau\cdot\sigma)(1)},x_{(\tau\cdot\sigma)(2)},\cdots,x_{(\tau\cdot\sigma)(n)})$

= $(\tau\cdot\sigma)\cdot f(x_1,x_2,\cdots,x_n)$

よって $(\tau\cdot(\sigma\cdot f))(x_1,x_2,\cdots,x_n)$ = $(\tau\cdot\sigma)\cdot f(x_1,x_2,\cdots,x_n)$ ■

●群の作用

群 G と集合 F があり、 $\sigma\in G$ と $x\in F$ に対して $y\in F$ が定まる時、 $y=\sigma\cdot x$ と書く。

すべての $\sigma,\tau\in G$ と $x\in F$ に対して

(1) G の単位元 e について $e\cdot x=x$

(2) $\tau\cdot(\sigma\cdot x)=(\tau\cdot\sigma)\cdot x$

が成立する時、 $\sigma\cdot x$ を群 G の**作用**(act)という。

$x_0\in F$ が任意の $\sigma\in G$ に対して $\sigma\cdot x_0=x_0$ ならば, x_0 を ***G* 不変**という。

●対象式

対称群 S_n 不変な関数は**対称式**または**対称関数**という。すなわち n 次のすべての置換 σ に対して

$f(x_1,x_2,\cdots,x_n)=f(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)})$ を満たす多項式(または,分数式)は対称式である。

補題より次の 2 点を満たすならば f は対称式である。

(1) $(1,2)f(x_1,x_2,\cdots x_{n-1},x_n)=f(x_1,x_2,\cdots,x_n)$

(2) $(12\cdots n)f(x_1,x_2,\cdots,x_n,x_n)=f(x_1,x_2,\cdots,x_n)$

●基本対象式

n 個の変数 $x_1,x_2,\cdots,x_n$ を解とする変数 T の多項式を展開してできる係数を $a_1,a_2,\ldots,a_n$ とする。

$(T-x_1)(T-x_2)\cdots(T-x_n)=T^n-a_1T^{n-1}+\cdots-(-1)^n a_n$

- $a_1=x_1+x_2+\cdots+x_n$
- $a_2=x_1x_2+x_1x_3+\cdots+x_{n-1}x_n$
- $a_n=x_1x_2\cdots x_n$

$a_1,a_2,\cdots,a_n$ は $x_1,x_2,\ldots,x_n$ の**基本対称式**という。2 次方程式の根と係数の関係の一般化である。

[**対称式の基本定理**] 対称式は基本対称式の四則演算の式で表せる。
[証明]
(1) 対称式が $x_1, x_2, \dots, x_n$ の多項式の時
3 変数 x, y, z の場合のみ証明する。対称多項式 $f(x,y,z)$ は n 次の斉次式、つまり f のすべての項は c を定数として $cx^i y^j z^k (x+y+z=n)$ であると仮定しても一般性を失わない。
もし $f(x,y,z)$ が $cx^i y^j z^k (x+y+z=n)$ の項を含むなら対称性より $i \geq j \geq k$ が成り立つとしてよい。
$x^i y^j z^k$ の指数 (i,j,k) ($(i+j+k=n, i \geq j \geq k)$)について $s=100i+10j+k$ 等により、大小を決める。
基本対称式を $p=x+y+z$ $q=xy+yz+zx$ $r=xyz$ とする。
[STEP1] $p^a q^b r^c$ の展開式の一般項は $cx^i y^j z^k$ ($i+j+k=a+2b+3c$) となることを以下に示す。
$a1+a2+a3=a$, $b1+b2+b3=b$ $c_1=\dfrac{a!}{a1!\,a2!\,a3!}$ $c_2=\dfrac{b!}{b1!\,b2!\,b3!}$ として、一般項は
$c_1 x^{a1} y^{a2} z^{a3} \times c_2 (xy)^{b1} (yz)^{b2} (zx)^{b3} \times x^c y^c z^c = c_1 c_2 x^{a1+b1+b3+c} y^{a2+b1+b2+c} z^{a3+b2+b3+c} = c_1 c_2 x^i y^j z^k$
ここで $i=a1+b1+b3+c$ $j=a2+b1+b2+c$ $k=a3+b2+b3+c$ である。この時 $i+j+k=a+2b+3c$
[STEP2] f_A の最大指数 (i,j,k) の項 $t = cx^i y^j z^k$ について、
c' を適当に定めることにより、 $f_B=f_A-c'p^{i-j}q^{j-k}r^k$ が t を含まないようにできることを以下に示す。
$i \geq j \geq k$ $(i-j)+2(j-k)+3k=i+j+k$ より、指数 (i,j,k) の項は $p^{i-j}q^{j-k}r^k$ 展開項の中にある。
それを $c''x^i y^j z^k$ とすると $c'=c/c''$ とすれば $f_B=f_A-c'p^{i-j}q^{j-k}r^k$ は項 t を含まない。

[STEP3]もし $f(x,y,z)$ が項 $c_1 x^n$ すなわち $(n,0,0)$ の項を含むなら $f_1=f-c'_1 p^n$ とおくと,
f_1 は項 $c_1 x^n$ すなわち指数 $(n,0,0)$ の項を含まない。
もし f_1 が項 $c_2 x^{n-1} y$ すなわち指数 $(n-1,1,0)$ の項を含むなら $n>1$ なので $f_2=f_1-c_2 p^{n-2} q$ とおくとこれは $x^{n-1} y$ すなわち指数 $(n-1,1,0)$ の項を含まない。
n を固定しているとき項は有限個なのでこの操作は有限回で終わる。
たとえば 4 次式の場合なら対称式 f から最初に $c_1 p^4$,次に $c_2 p^2 q$, $c_3 q^2$, $c_4 pr$ を順次引くことにより対称式 f は p, q, r の式で書かれる。
(2)対称式が $x_1, x_2, \dots, x_n$ の分数式の時
対称式 $h=\dfrac{f}{g}$ について f, g をすべて約分することにより, f と g は互いに素な多項式としてよい。
置換 $\sigma \in S_n$ に対して $\dfrac{\sigma f}{\sigma g}=\sigma \cdot h=h=\dfrac{f}{g}$ → $g(\sigma \cdot f)=f(\sigma \cdot g)$
f, g は互いに素だから f は $\sigma \cdot f$ の因子となり、同じ次数だから定数 $c(\sigma)$ により $\sigma \cdot f=c(\sigma) f$
さらに置換 τ を作用させると $\tau \cdot (\sigma \cdot f)=c(\sigma)(\tau \cdot f) = c(\sigma)c(\tau) f$ (A)
一方,置換の積と作用の関係式から $\tau \cdot (\sigma \cdot f)=(\tau \cdot \sigma) \cdot f=c(\tau \cdot \sigma) f$ (B)
(A)(B)および $f \neq 0$ なので $c(\tau \cdot \sigma)=c(\sigma)c(\tau)$
補題より、互換 τ について $c(\tau)^2=c(\tau^2)=c(e)=1$ だから $c(\tau)=\pm 1$ である。
(I) $c((1,2))=-1$ の時,すべての互換 τ について $c(\tau)=-1$ であり、 $\tau \cdot f=-f$ である。
よって f は交代式であって差積 $\triangle$ を因数に持つ。
同様にして g は交代式で差積 $\triangle$ を因数に持つので, f と g が互いに素という仮定に反する。
(ii) $c((1,2))=1$ の時、すべての互換 τ について $c(\tau)=1$ であり、 $\sigma \cdot f=f$ である。
よって f は対称式である。その結果 $g=\dfrac{f}{h}$ も対称式になる。
f と g は基本対称式で表せるので h も基本対称式で表される。■

●交代群

$x\in S$ に対して $Gx=\{\sigma|\sigma\cdot x=x\}$ とおくと G の部分群となる。これを $\boldsymbol{x}$ での**固定群**(stabilizer)という。

[例] $G=S_4$, $f(x_1,x_2,x_3,x_4)=x_1x_2+x_3x_4$ とおくとき f での固定群 Gf は

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

関数 $\triangle(x_1,x_2,\cdots,x_n)=\underset{j>i}{\Pi}(x_i-x_j)$ を**差積**と定義する。互換 τ を作用させると $\tau\cdot\triangle=-\triangle$

置換 σ を互換の積で表す時,それに必要な互換の個数を r とすると $\sigma\cdot\triangle=(-1)^r\triangle$

よって $(-1)^r$ は置換 σ のみで決まり、 r が偶数か奇数かは σ により決まる。

r が偶数のとき σ を**偶置換**、奇数のとき σ を**奇置換**という。

偶置換全体の集合 A_n は対称群 S_n の部分群であり、 $A_n=S_n\Delta=\{\sigma|\sigma\Delta=\Delta\}$ の意味で $\triangle$ での固定群である。これを**交代群**という。 $\triangle$ は交代群に対して不変である。

●交代式

任意の互換 τ について $\tau\cdot h=-h$ を満たす関数 h を**交代式**という。

[**定理**] 交代式 h は対称式 g と差積 Δ により $h=g\triangle$ と因数分解される。

[証明] 全ての互換について交代式の定義から $(i,j)h=-h$ (1)

$h(x_{1,}x_{2,}\cdots,x_n)$ に $x_i=x_j$ を代入すると $(i,j)h=h$ (2)

(1)(2)より $x_i=x_j$ の時、 $h=0$

因数定理より h は (x_i-x_j) を因数にもつ。以上から h は Δ を因数に持ち $h=g\triangle$ と書ける。

これにより $(i,j)h=(i,j)g\Delta=((i,j)g)((i,j)\Delta)=-((i,j)g)\Delta$ かつ $(i,j)h=-h=-g\Delta$ より

$((i,j)g)\Delta=g\Delta$ → $(i,j)g=g$ よって $\mathfrak{g}$ は対称式である。

[**定理**] 偶置換は 3 サイクルの積として表せる。

[証明] 2 個の互換の積は次の場合があり,いずれも 3 サイクルの積になる。

(A) $(1,2)(1,2)=e$

(B) $(1,3)(1,2)=(123)$

(C) $(3,4)(1,2)=((3,4)(1,3))((1,3)(1,2))=(143)(123)$

(B)について確かめると、

(1,3)(1,2)(1) = (1,3)(2) =(2)

(1,3)(1,2)(2) = (1,3)(1) =(3)

(1,3)(1,2)(3) = (1,3)(3) =(1)

上記の結果は相異なる $i_{1,}i_{2,}i_{3,}i_4$ でも成立する。よって、任意の偶置換は 3 サイクルの積で表せる。

●交換子

群の元である σ,τ について $[\sigma,\tau]$ = $\sigma^{-1}\tau^{-1}\sigma\tau$ を**交換子**という。

[**定理**] $n\geq5$ ならば、交代群 A_n は交換子の積で表せる。

[証明] 5 サイクル $\sigma=(12345)$ と 3 サイクル $\tau=(123)$ について $\sigma^{-1}=(15432),\tau^{-1}=(132)$ より

$\sigma^{-1}\tau^{-1}\sigma\tau(1)=\sigma^{-1}\tau^{-1}\sigma(2)=\sigma^{-1}\tau^{-1}(3)=\sigma^{-1}(2)=1$

$\sigma^{-1}\tau^{-1}\sigma\tau(2)=\sigma^{-1}\tau^{-1}\sigma(3)=\sigma^{-1}\tau^{-1}(4)=\sigma^{-1}(4)=3$

$\sigma^{-1}\tau^{-1}\sigma\tau(3)=\sigma^{-1}\tau^{-1}\sigma(1)=\sigma^{-1}\tau^{-1}(2)=\sigma^{-1}(1)=5$

$\sigma^{-1}\tau^{-1}\sigma\tau(4)=\sigma^{-1}\tau^{-1}\sigma(4)=\sigma^{-1}\tau^{-1}(5)=\sigma^{-1}(5)=4$

$\sigma^{-1}\tau^{-1}\sigma\tau(5)=\sigma^{-1}\tau^{-1}\sigma(5)=\sigma^{-1}\tau^{-1}(1)=\sigma^{-1}(3)=2$

以上より $[\sigma,\tau]$ = $\sigma^{-1}\tau^{-1}\sigma\tau=(235)$ この式は相異なる数 $i_{1,}i_{2,}i_{3,}i_{4,}i_5$ でも成立する。

よって 3 サイクル $(i_{1,}i_{4,}i_2)$ は交換子になる。交代群は 3 サイクルで生成されるので、交換子でも生成される。

■

§ 5次方程式の解の公式についてのアーベルの定理

体の定義の知識を前提とする。ここで方程式の係数は複素数の集合 C の要素とする。

2次方程式 $x^2-ax+b=0$ の解 α,β を係数 a,b で表した公式

$\alpha=\dfrac{a+\sqrt{a^2-4b}}{2}$　　$\beta=\dfrac{a-\sqrt{a^2-4b}}{2}$ および、解と係数の関係から $a=\alpha+\beta$　　$b=\alpha\beta$

これより、係数 a,b は解 α,β についての対称式になる。

これが公式として機能するためには α と β の間、 a と b の間に変数としての独立性が必要である。

また $F=a^2-4b$ は係数の四則演算の式であり、 $f=\sqrt{F}$ はそのべき根である。

C と係数 $\{a,b\}$ を含む最小の体を $K=C(a,b)$ ， K に $f=\sqrt{F}$ を付加した体 $K(f)$ とする。

[体と2次方程式の解との関係]

(1) $\alpha,\beta,f\notin K=C(a,b)$

(2) $\alpha,\beta\in K(f)$ この時、2次方程式の解は係数の四則演算とべき根で表せる。

[証明]

もし、解 α を a,b の四則演算の式で表せたと仮定すると、 $\alpha=h(a,b)$ と書ける。

この両辺に互換 $\tau=(\alpha,\beta)$ を作用させると $\beta=\tau\cdot\alpha=\tau\cdot h(a,b)=h(\tau\cdot a,\tau\cdot b)=h(a,b)=\alpha$

→ α と β の独立性に矛盾する。このことは $\alpha\notin K=C(a,b)$ であることを意味する。

もし、 $f\in K=C(a,b)$ と仮定すると、解の公式から $\alpha\in K=C(a,b)$ となり、これも矛盾を生ずる。

このことは $f\notin K=C(a,b)$ であることを意味する。 f は α と β の対称式では表せない。

また、解の公式より $\alpha,\beta\in K(f)$ ■

同じように、5次方程式の解をその係数で表す公式を考える。それは、その係数の四則演算とそのべき根によって構成されているので、体に係数とそのべき根を付加した体に含まれている。その四則演算を構成することにより、解の公式が導かれるはずである。

● n 次方程式の解と係数から体の構成へ

代数方程式 $T^n-a_1T^{n-1}+\cdots-(-1)^na_n=(T-x_1)(T-x_2)\cdots(T-x_n)$ において $x_1,x_2,\ldots,x_n$ は解を表す。

係数 $a_1,a_2,\cdots,a_n$ で表された解の公式の機能のためには $a_1,a_2,\cdots,a_n$ の代数的独立が必要である。

また $a_1,a_2,\cdots,a_n$ は $x_1,x_2,\ldots,x_n$ の基本対称式となる。

係数体を複素数体 C として， $K=C(a_1,a_2,\cdots,a_n)$　　$L=C(x_1,x_2,\cdots,x_n)$ を定義する。

この時 $K\subset L$ かつ $K\neq L$ が成り立つ。

[証明] $a_1,a_2,\cdots,a_n$ は $x_{1,}x_{2,}\ldots,x_n$ で表せるから $a_1,a_2,\cdots,a_n\in L=C(x_1,x_2,\cdots,x_n)$

→ $K=C(a_1,a_2,\cdots,a_n)\subset L$

もし $K=L$ と仮定すると、解 $x_1,x_2,\ldots,x_n$ は $a_1,a_2,\cdots,a_n$ の四則演算で表せる。

それを $x_i=h_i(a_1,a_2,\cdots,a_n)$　　$(i=1,2,\cdots,n)$　と表す。これに互換 $\tau=(i,j)$ を作用させると

$x_j=\tau\cdot x_i=\tau\cdot h_i(a_1,a_2,\cdots,a_n)=h_i(\tau\cdot a_1,\tau\cdot a_2,\cdots,\tau\cdot a_n)=h_i(a_1,a_2,\cdots,a_n)=x_i$ これは代数的独立に矛盾する。

対称群 S_n は有理関数の体 L に作用し,その S_n 不変体が $K=C(a_1,a_2,\cdots,a_n)$ となる。■

●問題の定式化

四則演算とべき根を組み合わせて解の公式を求めることは次のように定化できる。

$K_0=K$　　$K_N=L$ とおき、 $k\geq1$ として次のように体 K_k の漸化式を作る。

(1) $F_k\in K_{k-1}$ と素数 p_k を $f_k=\sqrt[p_k]{F_k}\notin K_{k-1}$ となるように選び、 $K_k=K_{k-1}(f_k)$ と定める。

(2) 解の公式が存在するための必十条件は、ある $k=N$ が存在して $L=K_N$ となることである。

すなわち $K_l\subset K_2\subset\cdots\subset K_N=L$

[アーベルの定理] 5次以上の代数方程式の解を、その係数の四則演算とべき根の式で表すことは不可能。
[証明]

[STEP1]　$p=p_1$ とすると $(\sigma\cdot f_1)^p=\sigma\cdot f_1^p=\sigma\cdot F_1=F_1=f_1^p$ → $\left(\dfrac{\sigma\cdot f_1}{f_1}\right)^p=1$

よって1の p 乗根 $c(\sigma)$ により $\sigma\cdot f_1=c(\sigma)f_1$ と書ける。
これより $(\tau\cdot\sigma)\cdot f_1=\tau\cdot(\sigma\cdot f_1)=\tau\cdot(c(\sigma)f_1)=c(\tau)(c(\sigma)f_1)=(c(\tau)c(\sigma))f_1$ → $c(\tau\cdot\sigma)=c(\tau)c(\sigma)$

補題より、互換 τ について $c(\tau)=\pm1$
もし $c((1,2))=1$ と仮定すると、補題よりすべての互換 τ について $c(\tau)=1$ なので $\sigma\cdot f_1=f_1$
よって f_1 は対称式であり、 $a_1,a_2,\cdots,a_n$ の式で表せるので、 $f_1\in K_0=K$
これは、 $f_1=\sqrt[p]{F_1}\notin K_0$ となるように F_1 を選んだことに矛盾する。
よって $c((1,2))=-1$ である。補題よりすべての互換 τ について $c(\tau)=-1$ なので $\tau\cdot f_1=-f_1$
f_1 は交代式であり、差積 △ と K の元 h を用いて $f_1=\triangle h$ と書ける。したがって
$K_1=K_0(f_1)=K(\triangle)$ は交代群 A_5 で不変な体であり、その元は偶置換で不変である。

[STEP2]　$q=p_2$ とおくと, $f_2^q=F_2\in K_1$ なので偶置換 σ に対して
$(\sigma\cdot f_2)^q=\sigma\cdot f_2^q=\sigma\cdot F_2=F_2=f_2^q$ → $\left(\dfrac{\sigma\cdot f_2}{f_2}\right)^q=1$
よって1の q 乗根 $c(\sigma)$ により $\sigma\cdot f_2=c(\sigma)f_2$ と書ける。
STEP1と同じ論法で $c(\sigma)$ は準同型となる。
$c(\sigma)c(\tau)=c(\tau)c(\sigma)$ より σ,τ の交換子 $[\sigma,\tau]=\sigma^{-1}\tau^{-1}\sigma\tau$ について
$c([\sigma,\tau])=c(\sigma^{-1}\tau^{-1}\sigma\tau)=c(\sigma^{-1})c(\tau^{-1})c(\sigma)c(\tau)=1$

ここで $n\geq5$ とする。 A_n の元は交換子の積で表せるので、
すべての $\sigma\in A_n$ について $c(\sigma)=1$ → $\sigma\cdot f_2=f_2$ → $f_2\in K_1$ → $K_2=K_1(f_2)=K_1$
以後、これを繰り返しても $K=K_0\subset K_1=\cdots=K_S\neq L$
したがって、5次以上の代数方程式の解の公式を構成することは不可能であり、存在しない。 ■

§ エピローグ/ガロアの理論への架け橋
拡大体と部分群の関係を確認する。
K を一般の体とし、全単射 $\delta:K\to K$ が次を満たすとき δ を K の自己同型写像という。
$\delta(f+g)=\delta(f)+\delta(g)$
$\delta(f\cdot g)=\delta(f)\cdot\delta(g)$
自己同型写像の集合 G は写像の合成で群となる。

G の部分群 H に対して集合 $K(H)$ をつぎのように定義すると、これは体になる。
$K(H)=\{f\in K|H$ 内のすべての自己同型写像 δ について $\delta(f)=f\}$
→ $H_1\subset H_2$ ならば $K(H_1)\supset K(H_2)$ (A)

対称式全体からなる体 $K=C(a_1,a_2,\cdots,a_n)$ に対して S_n は自己同型写像による群となる。
$S_n\supset A_n$ であり、 $K(S_n)=K\subset K(A_n)=K(\Delta)$ となっていた。
(A)によると $K(\Delta)$ にべき根を付加しても体は拡大しないことを A_n に適当な部分群がないことから証明することもできる。ガロアの理論でその証明を見ることができる。