入門　５次方程式の解法

Abel (1802-1829)

Galois (1811-1832)

Hermite (1822-1901)

Abel　：1826 年

「４次より高次の一般方程式の代数的解法の不可能性の証明」の論文により、５次以上の代数方程式は一般には四則演算とベキ根だけで(代数的に)解くことはできないことを示した。

Galois　：1831 年

「第 1 論文（le premier memoire）方程式論」
「第 2 論文（le second memoire）方程式論の応用」
これらの中で、方程式が四則演算とベキ根によって解けるための条件を考察し、その結果、一般の５次方程式は代数的に解けないことを示した。

Hermite　：1858 年

「Sur la resolution de l'equation du cinquieme degre」の論文により
５次方程式（詳しくは $x^5-x-a=0$ 型)の楕円モジュラー関数による「解の公式」を与えた。

〖内容〗

◇1 代数的可解性 (p3～p14)
一般には５次方程式を代数的(四則演算とベキ根だけを使う)に解くことはできないが、 F_{20} ,D_{10} ,C_5 をガロア群にもつ５次方程式は、 $F_{20} \supseteq D_{10} \supseteq C_5 \supseteq \{1\}$ を考えれば、 F_{20} 以下は可解群なのでこれをガロア群にもつ５次方程式は、代数的に解くことができる

◇2 ルンゲの定理 (p15～p17)
『 λ ,μ を有理数とするとき、
$x^5+\frac{5\mu^4(4\lambda+3)}{\lambda^2+1}x+\frac{4\mu^5(2\lambda+1)(4\lambda+3)}{\lambda^2+1}=0$ は代数的に解ける 』

◇3 エルミートによる解法 (p18～p22)
(例) S_5 をガロア群にもつ $x^5-80x+192=0$ の解（近似値）

◇4 代数的解法 (p23～p44)
(例 1) $x^5-20x^3-60x^2-70x-30=0$ の解
(例 2) $x^5-x^3-2x^2-2x-1=0$ の解
(例 3) $x^5+15x+44=0$ の解
(例 4) $x^5+20x+32=0$ の解
(例 5) $x^5-110x^3-55x^2+2310x+979=0$ の解

引用、参考文献 (p45)

◇1 代数的可解性

はじめに。

〔分解体〕

体 K 上(K 内の係数をもつ)既約な多項式$f(x)$ が K の拡大体 L 上で 1 次因数の積に分解するとき、L を$f(x)$ の K 上の分解体と言う。それら分解体の中で最小のものを最小分解体という。(分解体と言えば、これを指すことも多い)

たとえば、有理数体 Q 上既約な多項式 $f(x)=x^2-2$ の最小分解体は、$f(x)=\left(x+\sqrt{2}\right)\left(x-\sqrt{2}\right)$ となるので、有理数体Q に$\sqrt{2}$ を添加した拡大体 $Q\left(\sqrt{2}\right)=\left\{a+b\sqrt{2}\ \middle|\ a\,,b\ \in Q\right\}$ である。

複素数体 C は実数体 R 上の既約多項式 $f(x)=x^2+1$ の最小分解体になっていて、$C=R\left(\sqrt{-1}\right)=R(\,i\,)$ といえる。

〔ガロア拡大〕

体 K 上の既約な多項式$f(x)$ がその最小の分解体 L 内で相異なる 1 次因数の積に分解される(重解をもたない)とき、L を K のガロア拡大という。

(詳しくは、分離拡大であり正規拡大であるものをガロア拡大。)

たとえば、Q 上既約な $f(x)=x^2-2$ は、$Q\left(\sqrt{2}\right)$ 上で、$f(x)=\left(x+\sqrt{2}\right)\left(x-\sqrt{2}\right)$ なので $Q\left(\sqrt{2}\right)$ は、Q のガロア拡大。

Q 上既約な $f(x)=x^3-2$ は、$Q\left(\sqrt[3]{2}\,\right)=\{a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2\mid a\,,b\,,c\ \in Q\}$ 上では、$f(x)=\left(\ x-\sqrt[3]{2}\,\right)\left(x^2+\sqrt[3]{2}\,x+\left(\sqrt[3]{2}\right)^2\right)$ となるだけなので、$Q\left(\sqrt[3]{2}\right)$ は、Q のガロア拡大ではないが、Q が 1 の原始 3 乗根 ω を含んでいる$(\,Q\to Q(\omega)\,)$とすれば、

$\omega^3=1$, $\omega\neq1$, $\omega^2+\omega+1=0$ であって、

$$Q(\omega)\left(\sqrt[3]{2}\right)=Q\left(\omega\,,\sqrt[3]{2}\,\right)=\left\{s+t\sqrt[3]{2}+u\left(\sqrt[3]{2}\right)^2\ \middle|\ s\,,t\,,u\in Q(\omega)\,\right\}$$

$$=\left\{a+b\sqrt[3]{2}+c\left(\sqrt[3]{2}\right)^2+e\omega+f\omega\sqrt[3]{2}+g\omega\left(\sqrt[3]{2}\right)^2\ \middle|\ a,b,c\,,e\,,f\,,g\in Q\,\right\}$$ 上では、

$f(x)=\left(x-\sqrt[3]{2}\right)\left(\,x-\sqrt[3]{2}\,\omega\right)\left(x-\sqrt[3]{2}\,\omega^2\right)$ となるので、$Q\left(\omega\,,\sqrt[3]{2}\,\right)$ は、Q のガロア拡大。

なお、$f(x)=x^3-2$ は、$Q(\omega)$上でも既約であり、$Q\left(\omega\,,\sqrt[3]{2}\,\right)$ は、$Q\,(\omega)$のガロア拡大。

〔自己同型写像〕

K を体とする。K からそれ自身への(全単射な)写像 σ があって、$\alpha\,,\beta\ \in K$ としたとき、 $\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$,$\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$ を満たすものを自己同型写像という。自己同型写像全体からなる集合は、写像の合成で積を定義すれば、群をなす。これを K の自己同型群といい、 $Aut(K)$ で表す。

たとえば、

$Q(\sqrt{2})=\{a+b\sqrt{2}\ |\ a,b\ \in Q\}$ からそれ自身への自己同型写像を σ とすると、

$Q(\sqrt{2})$ の任意の元 $a+b\sqrt{2}$ （$a,b\ \in Q$）に対し、

$\sigma(a+b\sqrt{2})=\sigma(a)+\sigma(b\sqrt{2})=a+b\sigma(\sqrt{2})$　(*)

ここで、$\sigma(\sqrt{2})^2=\sigma(\sqrt{2})\sigma(\sqrt{2})=\sigma(\sqrt{2}\sqrt{2})=\sigma(2)=2$

∴　$\sigma(\sqrt{2})=\pm\sqrt{2}$

∴　$\sigma(a+b\sqrt{2})=a+b\sqrt{2}$ または $a-b\sqrt{2}$

これより、σ としては、

i：　$a+b\sqrt{2}\ \rightarrow\ a+b\sqrt{2}\quad (a,b\ \in Q)$　　(単に$\sqrt{2}\rightarrow\sqrt{2}$ と略記)

σ：　$a+b\sqrt{2}\ \rightarrow\ a-b\sqrt{2}\quad (a,b\ \in Q)$　　(単に$\sqrt{2}\rightarrow-\sqrt{2}$ と略記)

$\{i\ ,\ \sigma\}$ が $Q(\sqrt{2})$ の自己同型群 $Aut(Q(\sqrt{2}))$である。

(*)　定義から $\sigma(0)=0$　,$\sigma(1)=1$ であり

有理数体 Q の元 a に対しては $\sigma(a)=a$ (不変)。

〔ガロア群〕

LをKの拡大体とするとき、Lの自己同型写像のうち、Kの元を不変にするものは、$Aut(L)$ の部分群をなすが、これを L の K上のガロア群といい、$G(L/K)$で表す。すなわち、$G(L/K)=\{\phi\in Aut(L)\ |\ \phi(a)=a\ ,a\in K\}$

Q の元は、どんな自己同型写像でも不変だから、$G(L/Q)=Aut(L)$

また、体 K上既約な$f(x)$の最小分解体を L としたとき、L のK上のガロア群 $G(L/K)$を多項式$f(x)$ (または方程式$f(x)=0$)のガロア群という。

たとえば、1 の原始 3 乗根を ω として、$L=Q(\omega,\sqrt[3]{2})$,$K=Q$ としたとき、

L の自己同型写像 σ としては、$\{\sigma(\sqrt[3]{2})\}^3=\sigma(2)=2$ より、$\sigma(\sqrt[3]{2})=\sqrt[3]{2}$,$\sqrt[3]{2}\,\omega$,$\sqrt[3]{2}\,\omega^2$

$\{\sigma(\omega)\}^3=\sigma(1)=1$ より、$\sigma(\omega)=\omega$, ω^2　($\because$ $\sigma(\omega)\neq 1$) を考慮すると

以下の 6 通りが考えられる。

$\sigma_0=i$ ： $\sqrt[3]{2}\ \rightarrow\sqrt[3]{2}$　　,$\omega\ \rightarrow\ \omega$　(恒等写像)

$\sigma_1=\sigma$ ： $\sqrt[3]{2}\ \rightarrow\sqrt[3]{2}\,\omega$　　,$\omega\ \rightarrow\ \omega$

$\sigma_2=\sigma^2$ ： $\sqrt[3]{2}\ \rightarrow\sqrt[3]{2}\,\omega^2$　,$\omega\ \rightarrow\ \omega$

$\sigma_3=\tau$ ： $\sqrt[3]{2}\ \rightarrow\sqrt[3]{2}$　　,$\omega\ \rightarrow\ \omega^2$

$\sigma_4=\tau\sigma$ ： $\sqrt[3]{2}\ \rightarrow\sqrt[3]{2}\,\omega^2$　,$\omega\ \rightarrow\ \omega^2$

$\sigma_5=\tau\sigma^2$ ： $\sqrt[3]{2}\ \rightarrow\sqrt[3]{2}\,\omega$　,$\omega\ \rightarrow\ \omega^2$

$Aut(L)=G(L/K)=\{\,i,\sigma,\sigma^2,\tau\ ,\tau\sigma\ ,\tau\sigma^2\}$

ここで、　$K_1=Q(\omega)$　,$K_2=Q(\sqrt[3]{2})$ とすると

$Aut(L)$ の中で、$Q(\omega)$ の元を不変にするものは、$\{\,i,\sigma,\sigma^2\}$であり、

$G(L/K_1)=\{\,i,\sigma,\sigma^2\}$ 。また、$Q(\sqrt[3]{2})$ の元を不変にするものは、

$\{\,i,\tau\}$であり、$G(L/K_2)=\{\,i,\tau\}$ 。

〔ガロアの基本定理=ガロア拡大とガロア群の関係〕

① L が Q のガロア拡大のとき、ガロア群 $G=G(L/Q)$ の部分群 H_1 , H_2 には
それぞれ、不変体 M_1 , M_2 が(逆向きに) $1:1$ に対応する。

$Q \subset M_1\ (M_2) \subset L$

$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$

$G \subset H_1\ (H_2) \subset \{i\}$

② L が Q のガロア拡大のとき、L は $M_1\ (M_2)$ のガロア拡大となり、

$[L:Q]=|G(L/Q)=|G|$

$[L:M_1]=|G(L/M_1)=|H_1|$

$[L:M_2]=|G(L/M_2)=|H_2|$

$\uparrow \qquad \uparrow$

拡大次数　　位数

たとえば、

$L=Q(\omega,\sqrt[3]{2})$ (1 の原始 3 乗根を ω) とし、$M_1=Q(\omega)$, $M_2=Q(\sqrt[3]{2})$ としたとき、

「σ: $\sqrt[3]{2} \rightarrow \sqrt[3]{2}\,\omega$, $\omega \rightarrow \omega$ 」,「τ: $\sqrt[3]{2} \rightarrow \sqrt[3]{2}$, $\omega \rightarrow \omega^2$」とすれば

$G(L/Q)=\{i,\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\}$ 　$[L:Q]=|G(L/Q)=|G|=6$

$G(L/M_1)=\{i,\sigma,\sigma^2\}=H_1$ 　$[L:M_1]=|G(L/M_1)=|H_1|=3$

$G(L/M_2)=\{i,\tau\}=H_2$ 　$[L:M_2]=|G(L/M_2)=|H_2|=2$

〔巡回群と巡回拡大〕

<巡回群>

たった 1 つの元 a から生成される群のことで、$<a>$ などと表す。

$<a>=\{\cdots\cdots a^{-3},a^{-2},a^{-1},i,a,a^2,a^3,\cdots\cdots\}$

(*i は恒等写像、a^{-2} は a^{-1} を 2 回、a^3 は* a を 3 回演算することを意味する)

$A_3=\left\{\begin{pmatrix}123\\123\end{pmatrix},\begin{pmatrix}123\\231\end{pmatrix},\begin{pmatrix}123\\312\end{pmatrix}\right\}=\{i,\sigma,\sigma^2\}$ は、

位数 3 の巡回群で 、$<\sigma>$と書ける。

<巡回拡大>

ガロア群が巡回群になるようなガロア拡大のことをいう。

1 の原始 3 乗根を ω としたとき、($\omega^3=1$, $\omega\neq 1$, $\omega^2+\omega+1=0$)

Q 上の既約多項式 $f(x)=x^2+x+1=0$ は、

$Q(\omega)=\{a+b\omega \mid a,b \in Q\}$ 上で、$f(x)=(x-\omega)(x-\omega^2)$ と分解

されるので、$Q(\omega)$ は、Q のガロア拡大であり、さらに

そのガロア群 $G(Q(\omega)/Q)$ としては、$\sigma(\omega)^3=1$より、

$\sigma(\omega)=\omega$, ω^2 $(\sigma(\omega)\neq 1)$ なので、

$\sigma_0 = i$ ： $\omega \ \rightarrow \ \omega$

$\sigma_1 = \sigma$ ： $\omega \ \rightarrow \ \omega^2$ が考えられ、$G(Q(\omega)/Q) = \{\, i \ , \sigma \,\}$ (位数２の巡回群)

したがって、$Q(\omega)$ は、Q の巡回拡大。

〔ベキ根拡大〕

体 F 上の既約多項式 $f(x) = x^n - a = 0$ の根(解)をベキ根(累乗根)という。

F が１の原始 n 乗根 ζ を含んでいるとき、F に１つのベキ根 $\sqrt[n]{a}$ $(a \in F)$ を添加した体 $F\left(\sqrt[n]{a}\right)$ を F のベキ根拡大という。

このとき、$F\left(\sqrt[n]{a}\right)$ は F の巡回拡大でもある。

ω を１の原始３乗根とし、$F = Q(\omega)$ とすれば、$F\left(\sqrt[3]{2}\right) = Q\left(\omega, \sqrt[3]{2}\right)$ は、F のベキ根拡大であり、ガロア拡大でもあるし巡回拡大でもある。

〔可解群〕

G を群とする。

G の部分群の減少列、$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots\cdots\cdots \supseteq G_r = \{\, 1 \,\}$ =(単位群)が

あって、G_{i+1} は G_i の正規部分群(*)で、剰余群(**) $G_{i+1}/\,G_i$ が可換群

(巡回群)となっているとき、G を可解群という。

(*) H が G の正規部分群とは、H が G の部分群で任意の $\sigma \in G$ に対し、
$\sigma H = H\sigma$ が成り立つことである。このことの代わりに
『$\sigma \in G$, $x \in H$ ならば、$\sigma x \sigma^{-1} \in H$ が成り立つとき』としてもよい

$S_3 = \left\{ \begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\231\end{pmatrix}, \begin{pmatrix}123\\312\end{pmatrix}, \begin{pmatrix}123\\132\end{pmatrix}, \begin{pmatrix}123\\321\end{pmatrix}, \begin{pmatrix}123\\213\end{pmatrix} \right\}$ (３次対称群)の

部分群、$A_3 = \left\{ \begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\231\end{pmatrix}, \begin{pmatrix}123\\312\end{pmatrix} \right\}$ (３次交代群)は、

S_3 の正規部分群である。

このことは、たとえば、$\tau = \begin{pmatrix}123\\132\end{pmatrix} \in S_3$ に対して

$$\tau\begin{pmatrix}123\\123\end{pmatrix} = \begin{pmatrix}123\\132\end{pmatrix}\begin{pmatrix}123\\123\end{pmatrix} = \begin{pmatrix}123\\132\end{pmatrix} \quad , \begin{pmatrix}123\\123\end{pmatrix}\tau = \begin{pmatrix}123\\132\end{pmatrix}$$

$$\tau\begin{pmatrix}123\\231\end{pmatrix} = \begin{pmatrix}123\\132\end{pmatrix}\begin{pmatrix}123\\231\end{pmatrix} = \begin{pmatrix}123\\321\end{pmatrix} \quad , \begin{pmatrix}123\\231\end{pmatrix}\tau = \begin{pmatrix}123\\213\end{pmatrix}$$

$$\tau\begin{pmatrix}123\\312\end{pmatrix} = \begin{pmatrix}123\\132\end{pmatrix}\begin{pmatrix}123\\312\end{pmatrix} = \begin{pmatrix}123\\213\end{pmatrix} \quad , \begin{pmatrix}123\\312\end{pmatrix}\tau = \begin{pmatrix}123\\321\end{pmatrix}$$

$\therefore \quad \tau A_3 = A_3 \tau$ (記号=は、集合として等しいことを意味する)

(**) 剰余群（商群）

H が G の正規部分群であるとき、G のH に対する商集合、

$G/H=\{gH \mid g\in G\}$ は、演算 $(g_1H)(g_2H)=(g_1g_2)H$

(ただし、g_1 ,$g_2\in G$)によって群となる。

これをG のH による剰余群（商群）という。

たとえば、S_3 とA_3 において、$\sigma=\begin{pmatrix}123\\231\end{pmatrix}$ $\tau=\begin{pmatrix}123\\132\end{pmatrix}$ とおくと、

$G=S_3=\{i,\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\}$, $H=A_3=\{i,\sigma,\sigma^2\}$ であり

$G/H=\{H\ ,\tau H\}$ である。(G/H の単位元は H である)

＜可解群の例＞

① 可換群 G は、可解群である。

$G\supseteq\{1\}$ の部分群列を考えればよい

② S_3 (３次対称群)は、可解群である。

$S_3\supseteq A_3\supseteq\{1\}$ (A_3は３次交代群)を考えればよい

A_3 は S_3 の、$\{1\}$ は A_3のそれぞれ正規部分群であり、

S_3/A_3 は、位数２の巡回群で、$A_3/\{1\}=A_3$ は、位数３の巡回群でいずれも可換群。

③ S_4 (４次対称群)は、可解群である。

$S_4\supseteq A_4\supseteq V\supseteq\{1\}$ (A_4は４次交代群)を考えればよい

ここで、

$$A_4=\{\begin{pmatrix}1234\\1234\end{pmatrix},\begin{pmatrix}1234\\2314\end{pmatrix},\begin{pmatrix}1234\\3124\end{pmatrix},\begin{pmatrix}1234\\2431\end{pmatrix},\begin{pmatrix}1234\\4132\end{pmatrix},\begin{pmatrix}1234\\3241\end{pmatrix},$$

$$\begin{pmatrix}1234\\4213\end{pmatrix},\begin{pmatrix}1234\\1342\end{pmatrix},\begin{pmatrix}1234\\1423\end{pmatrix},\begin{pmatrix}1234\\2143\end{pmatrix},\begin{pmatrix}1234\\3412\end{pmatrix},\begin{pmatrix}1234\\4321\end{pmatrix}\}$$

$=\{\ i\ ,(1\ 2\ 3),(1\ 3\ 2),(1\ 2\ 4),(1\ 4\ 2),(1\ 3\ 4),$

$(1\ 4\ 3),(2\ 3\ 4),(2\ 4\ 3),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$

$=\{\ i\ ,\ (k\ l\ m)\ ,\ (k\ l)(m\ n)\}$ (ただしk,l,m,nは異なる１～４の数)

$S_4=\{\ A_4\ ,\ (1\,2),\ (1\,3),\ (1\,4),\ (2\,3),\ (2\,4),\ (3\,4),$

$(1\,2\,3\,4),(1\,2\,4\,3),(1\,3\,2\,4),(1\,3\,4\,2),(1\,4\,2\,3),(1\,4\,3\,2)\ \}$

$=\{A_4\ ,\ (k\ l),\ \ (k\ l\ m\ n)\}$

$$V=\left\{\begin{pmatrix}1234\\1234\end{pmatrix},\begin{pmatrix}1234\\2143\end{pmatrix},\begin{pmatrix}1234\\3412\end{pmatrix},\begin{pmatrix}1234\\4321\end{pmatrix}\right\}$$ ($Klein$の４元群)

$=\{\ i\ ,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$

$=\{\ i\ ,\ (k\ l)(m\ n)\ \}$

次のことなどから、A_4 は S_4 の正規部分群で、V は、A_4の正規部分群である。

“ $(k\ n)$, $(k\ l\ m\ n) \in S_4$,$(k\ l\ m) \in A_4$ に対し、

$(k\ n)^{-1}(k\ l\ m)(k\ n) = (l\ m\ n) \in A_4$

$(k\ l\ m\ n)^{-1}(k\ l\ m)(k\ l\ m\ n) = (k\ l\ n) \in A_4$ “

“ $(k\ l\ m) \in A_4$,$(k\ l)(m\ n) \in V$ に対し、

$(k\ l\ m)^{-1}(k\ l)(m\ n)(k\ l\ m) = (k\ m)(l\ n) \in V$ “

また、

$S_4/A_4 = \{\ A_4\ ,(1\ 2)A_4\ \}$,$A_4/V = \{\ V\ ,(1\ 2\ 3)V\ ,(1\ 3\ 2)V\ \}$

なので、S_4/A_4 は、位数 2 の巡回群(可換群)で、

A_4/V は、位数 3 の巡回群(可換群)。

$V/\{1\} = V$ は、位数 4 の可換群

④ p を素数としたとき、

群 G の位数 p であるならば、G は巡回群、従って可換群

であって可解群である。

ここから、<u>代数的可解性</u>

有理数体 Q 内に係数をもつ(Q 上の)既約方程式 $f(x) = 0$ が『代数的に可解である』とは、$f(x) = 0$ の係数に加減乗除とベキ根(累乗根)を有限回施して、$f(x) = 0$ の根(解)が得られることであり、それらの根が、それらの根を形作るベキ根をすべて含む体に含まれることである。

言い換えると、

Q 上の既約多項式 $f(x)$ において、Q から始まるベキ根拡大列

$Q = Q_0 \subseteq Q_1 \subseteq Q_2 \subseteq \cdots\cdots \subseteq Q_r = \Omega$ （Q_{i+1} は Q_i のベキ根拡大）があって

$f(x)$ の分解体 L が Ω に含まれることである。

たとえば、

Q 上の既約方程式 $f(x) = x^6 - 10x^3 + 23 = (x^3 - 5)^2 - 2 = 0$ は、Q 内に根(解)を持たないが、$\alpha^2 = 2$,$\beta^3 = 5 + \alpha$ としたとき、$Q(\alpha\ ,\beta)$ 内で、解

$x = \sqrt[3]{5 \pm \sqrt{2}}$,$\sqrt[3]{5 \pm \sqrt{2}} \cdot \omega$,$\sqrt[3]{5 \pm \sqrt{2}} \cdot \omega^2$ を持つ。

このとき、Q が 1 の原始 3 乗根 ω を含んでいるとして、($Q(\omega) \to Q$)

ベキ根拡大の列、$Q \subseteq Q(\alpha) \subseteq Q(\alpha\ ,\beta) = \Omega$ が得られ、

当然、$f(x)$ の分解体 $Q(\alpha\ ,\beta) = L \subseteq \Omega$ である。

〔ガロアの定理〕

〖 $f(x)$ を Q 上の既約多項式、 L を$f(x)$ の分解体とし、$G = G(L/Q)$ を $f(x)$ のガロア群とするとき、$f(x) = 0$ が四則演算とベキ根で解ける(代数的に可解である)ための必要十分条件は、G が可解群となることである。〗

A_5 は単純群(正規部分群として、それ自身と単位群$\{1\}$ しかもたない群)

であることから、S_5 の部分群列は、$S_5 \supseteq A_5 \supseteq \{1\}$ となるが、

$A_5 = A_5/\{1\}$ は可換群ではない(*)

したがって、S_5 は可解群でない。

(*) 反例をあげると、 $A_5 \ni \sigma = (1\ 2\ 3),\ \tau = (1\,2\,3\,4\,5)$ に対し

$\sigma\tau = (1\,2\,3)(1\,2\,3\,4\,5) = (\,1\,3\,4\,5\,2)$

$\tau\sigma = (1\,2\,3\,4\,5)(1\,2\,3) = (1\,3\,2\,4\,5)$ $\therefore\quad \sigma\tau \neq \tau\sigma$

これより、一般には５次方程式を四則演算とベキ根だけを使って解くことはできないが、以下の F_{20} ,D_{10} ,C_5 (**)をガロア群にもつ５次方程式は、 $F_{20} \supseteq D_{10} \supseteq C_5 \supseteq \{1\}$ を考えれば、

$F_{20}/D_{10} = \{D_{10}\ ,(2\,3\,5\,4)D_{10}\}$ $(2\,3\,5\,4)=\begin{pmatrix}12345\\13524\end{pmatrix}$ ∈奇置換

$D_{10}/C_5 = \{C_5\ ,(2\,5)(3\,4)C_5\}$ $(2\,5)(3\,4) = \begin{pmatrix}12345\\15432\end{pmatrix}$ ∈偶置換

であって、F_{20} 以下は、可解群であって、四則演算とベキ根だけを使って解くことができる。

(**) F_{20} … 位数 20 の群

$$\{\begin{pmatrix}12345\\12345\end{pmatrix}\ \begin{pmatrix}12345\\23451\end{pmatrix}\ \begin{pmatrix}12345\\34512\end{pmatrix}\ \begin{pmatrix}12345\\45123\end{pmatrix}\ \begin{pmatrix}12345\\51234\end{pmatrix}$$

$$\begin{pmatrix}12345\\15432\end{pmatrix}\ \begin{pmatrix}12345\\32154\end{pmatrix}\ \begin{pmatrix}12345\\54321\end{pmatrix}\ \begin{pmatrix}12345\\21543\end{pmatrix}\ \begin{pmatrix}12345\\43215\end{pmatrix}$$

$$\begin{pmatrix}12345\\13524\end{pmatrix}\ \begin{pmatrix}12345\\24135\end{pmatrix}\ \begin{pmatrix}12345\\35241\end{pmatrix}\ \begin{pmatrix}12345\\41352\end{pmatrix}\ \begin{pmatrix}12345\\52413\end{pmatrix}$$

$$\begin{pmatrix}12345\\14253\end{pmatrix}\ \begin{pmatrix}12345\\25314\end{pmatrix}\ \begin{pmatrix}12345\\31425\end{pmatrix}\ \begin{pmatrix}12345\\42531\end{pmatrix}\ \begin{pmatrix}12345\\53142\end{pmatrix}\}$$

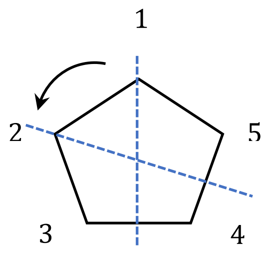
これは、置換 $\sigma = \begin{pmatrix}12345\\23451\end{pmatrix}$ と $\tau = \begin{pmatrix}12345\\13524\end{pmatrix}$ よって生成される群で

実際に $\{\ i\ ,\sigma\ ,\sigma^2\ ,\sigma^3\ ,\sigma^4,\ \tau\ ,\tau^2\ ,\tau^3\ ,\tau\sigma\ ,\tau\sigma^2,\tau\sigma^3,\tau\sigma^4\ ,$

$\tau^2\sigma$,$\tau^2\sigma^2$,$\tau^2\sigma^3$,$\tau^2\sigma^4$,$\tau^3\sigma$,$\tau^3\sigma^2$,$\tau^3\sigma^3$,$\tau^3\sigma^4$ } である。

D_{10} … 位数 10 の群

これは正五角形の回転や鏡映によって得られるもの。



$$\left\{\begin{pmatrix}12345\\12345\end{pmatrix}\ \begin{pmatrix}12345\\23451\end{pmatrix}\ \begin{pmatrix}12345\\34512\end{pmatrix}\ \begin{pmatrix}12345\\45123\end{pmatrix}\ \begin{pmatrix}12345\\51234\end{pmatrix}\right.$$

$$\left.\begin{pmatrix}12345\\15432\end{pmatrix}\ \begin{pmatrix}12345\\32154\end{pmatrix}\ \begin{pmatrix}12345\\54321\end{pmatrix}\ \begin{pmatrix}12345\\21543\end{pmatrix}\ \begin{pmatrix}12345\\43215\end{pmatrix}\right\}$$

C_5 … 位数 5 の巡回群

$$\left\{\begin{pmatrix}12345\\12345\end{pmatrix}\ \begin{pmatrix}12345\\23451\end{pmatrix}\ \begin{pmatrix}12345\\34512\end{pmatrix}\ \begin{pmatrix}12345\\45123\end{pmatrix}\ \begin{pmatrix}12345\\51234\end{pmatrix}\right\}$$

C_5 やF_{20} をガロア群にもつ 5 次方程式の解

① C_5 をガロア群にもつ、

$f(x) = x^5 + x^4 - 12x^3 - 21x^2 + x + 5 = 0$ （#） の解

$f(x) \equiv (x+25)^5 \quad (mod\ 31)$ となることを踏まえて。

1 の原始 31 乗根を ζ としたとき、(つまり、$\zeta^{31} = 1$,$\zeta \neq 1$ より

$\zeta^{30} + \zeta^{29} + \cdots\cdots + \zeta + 1 = 0$ ） $Q(\zeta)$ の Q 上のガロア群 $G = G(Q(\zeta)/Q)$ は

位数 30 の巡回群である。すなわち、

σ ： $\zeta \to \zeta^3$,$\zeta^2 \to \zeta^6$,$\zeta^3 \to \zeta^9$,$\zeta^4 \to \zeta^{12}$,$\zeta^5 \to \zeta^{15}$

$\zeta^6 \to \zeta^{18}$,$\zeta^7 \to \zeta^{21}$,$\zeta^8 \to \zeta^{24}$,$\zeta^9 \to \zeta^{27}$,$\zeta^{10} \to \zeta^{30}$

$\zeta^{11} \to \zeta^2$,$\zeta^{12} \to \zeta^5$,$\zeta^{13} \to \zeta^8$,$\zeta^{14} \to \zeta^{11}$,$\zeta^{15} \to \zeta^{14}$

$\zeta^{16} \to \zeta^{17}$,$\zeta^{17} \to \zeta^{20}$,$\zeta^{18} \to \zeta^{23}$,$\zeta^{19} \to \zeta^{26}$,$\zeta^{20} \to \zeta^{29}$

$\zeta^{21} \to \zeta$,$\zeta^{22} \to \zeta^4$,$\zeta^{23} \to \zeta^7$,$\zeta^{24} \to \zeta^{10}$,$\zeta^{25} \to \zeta^{13}$

$\zeta^{26} \to \zeta^{16}$,$\zeta^{27} \to \zeta^{19}$,$\zeta^{28} \to \zeta^{22}$,$\zeta^{29} \to \zeta^{25}$,$\zeta^{30} \to \zeta^{28}$

とすれば、

$G = \{ i\ ,\sigma\ ,\sigma^2 ,\sigma^3 , \ldots\ldots\ldots\ldots, \sigma^{29} \} \qquad (\sigma^{30} = i)$

このうち､、位数が 6 となる部分群は、

$H = \{\, i\ ,\sigma^5\ ,\sigma^{10}\ \ ,\sigma^{15}\ \ ,\sigma^{20}\ \ ,\sigma^{25}\ \}$だけで

これに対応する $Q(\zeta)$ と Q の中間体を M とすれば

G は、巡回群だからその部分群 H も巡回群で

可換である(ゆえにHはGの正規部分群) から

M は Q の 5 次の巡回拡大である。

$$\left.\begin{array}{ccc} Q(\zeta) & \dots & \{i\} \\ 6| & & 6| \\ M & \dots & H \\ 5| & & 5| \\ Q & \dots & G \end{array}\right]\ 30$$

$f(x) = 0$ の 1 つの解を α とすれば、$M = Q(\alpha)$ (H による不変体)であり

$\alpha = i(\zeta) + \sigma^5(\zeta) + \sigma^{10}(\zeta) + \sigma^{15}(\zeta) + \sigma^{20}(\zeta) + \sigma^{25}(\zeta)$

$\quad = \zeta + \zeta^{26} + \zeta^{25} + \zeta^{30} + \zeta^5 + \zeta^6$

$\quad = \zeta + \zeta^5 + \zeta^6 + \zeta^{25} + \zeta^{26} + \zeta^{30} \quad (= \alpha_1)$

他の解は、

$\sigma(\alpha_1) = \zeta^3 + \zeta^{15} + \zeta^{18} + \zeta^{13} + \zeta^{16} + \zeta^{28}\ \ (= \alpha_2)$

$\sigma(\alpha_2) = \zeta^9 + \zeta^{14} + \zeta^{23} + \zeta^8 + \zeta^{17} + \zeta^{22}\ \ (= \alpha_3)$

$\sigma(\alpha_3) = \zeta^{27} + \zeta^{11} + \zeta^7 + \zeta^{24} + \zeta^{20} + \zeta^4\ \ (= \alpha_4)$

$\sigma(\alpha_4) = \zeta^{19} + \zeta^2 + \zeta^{21} + \zeta^{10} + \zeta^{29} + \zeta^{12}\ \ (= \alpha_5)$

(#) 巡回群 C_5をもつこの方程式の作り方

1 の原始 31 乗根を ζ としたとき、

$Q(\zeta)$ の Q 上ガロア群 $G = G(Q(\zeta)/Q)$ は位数 30 の巡回群で

あり、 $\sigma\ :\ \zeta \to \zeta^3\ ,\zeta^2 \to \zeta^6\ \ ,\cdots\cdots\cdots,\zeta^{29} \to \zeta^{25},\zeta^{30} \to \zeta^{28}$

とすれば、$G = \{\, i\ ,\sigma\ \ ,\sigma^2\ ,\sigma^3\ ,\dots\dots\dots\dots,\sigma^{29}\}\qquad (\sigma^{30} = i)$

このうち､、位数が 6 となる部分群は、

$H = \{\, i\ ,\sigma^5\ ,\sigma^{10}\ \ ,\sigma^{15}\ \ ,\sigma^{20}\ \ ,\sigma^{25}\ \}$だけで

これに対応する $Q(\zeta)$ と Q の中間体を M とすれば

G は、巡回群だからその部分群 H も巡回群で

可換である(ゆえにHはGの正規部分群) から

M は Q の 5 次の巡回拡大である。

$$\begin{array}{ccc} Q(\zeta) & \dots & \{i\} \\ 6| & & 6| \\ M & \dots & H \\ 5| & & 5| \\ Q & \dots & G \end{array}$$

また、

$\eta_1 = i(\zeta) + \sigma^5(\zeta) + \sigma^{10}(\zeta) + \sigma^{15}(\zeta) + \sigma^{20}(\zeta) + \sigma^{25}(\zeta)$

$\quad = \zeta + \zeta^{26} + \zeta^{25} + \zeta^{30} + \zeta^5 + \zeta^6$

$\quad = \zeta + \zeta^5 + \zeta^6 + \zeta^{25} + \zeta^{26} + \zeta^{30}\ \ (= \alpha_1\ )$

とすれば、$M = Q(\eta_1)$ (H による不変体)であり、η_1 と次の

$\eta_2 = \sigma(\eta_1) = \zeta^3 + \zeta^{15} + \zeta^{18} + \zeta^{13} + \zeta^{16} + \zeta^{28}\ \ (= \alpha_2)$

$\eta_3 = \sigma(\eta_2) = \zeta^9 + \zeta^{14} + \zeta^{23} + \zeta^8 + \zeta^{17} + \zeta^{22}\ \ (= \alpha_3)$

$\eta_4 = \sigma(\eta_3) = \zeta^{27} + \zeta^{11} + \zeta^7 + \zeta^{24} + \zeta^{20} + \zeta^4\ \ (= \alpha_4)$

$\eta_5 = \sigma(\eta_4) = \zeta^{19} + \zeta^2 + \zeta^{21} + \zeta^{10} + \zeta^{29} + \zeta^{12}\ \ (= \alpha_5)$ は、

M の Q 上の正規底(*)である。

η_1 のQ 上の次数が最小の多項式$f(x)$は、$(M/Q)=5$ であるから $f(x)$ の次数は 5 であり、

$f(x)=(x-\eta_1)(x-\eta_2)(x-\eta_3)(x-\eta_4)(x-\eta_5)$

ここで、コンピューターの助けを借りると

$\eta_1+\eta_2+\eta_3+\eta_4+\eta_5=-1$

$\eta_1\eta_2+\eta_1\eta_3+\cdots\cdots\cdots\cdots+\eta_4\eta_5=-12$

$\eta_1\eta_2\eta_3+\eta_1\eta_2\eta_4+\cdots\cdots\cdots\cdots+\eta_3\eta_4\eta_5=21$

$\eta_1\eta_2\eta_3\eta_4+\eta_1\eta_2\eta_3\eta_5+\cdots\cdots\cdots\cdots+\eta_2\eta_3\eta_4\eta_5=1$

$\eta_1\eta_2\eta_3\eta_4\eta_5=-5$

$\therefore\ f(x)=x^5+x^4-12x^3-21x^2+x+5$

これで式が作れた。

なお、 $f(x)$ のガロア群 $G=G(M/Q)=G(Q(\eta_1)/Q)$ は、

先の $Q(\zeta)$の自己同型写像 σ を $Q(\eta_1)$上に制限した

σ ： $\eta_1\to\eta_2$,$\eta_2\to\eta_3$,$\eta_3\to\eta_4$,$\eta_4\to\eta_5$,$\eta_5\to\eta_1$

によって、$G=\{\,i\ ,\sigma\ ,\sigma^2\ ,\sigma^3\ ,\sigma^4\ \}\cong C_5$

(*) 正規底

M が Q のガロア拡大であるとし、そのガロア群を $G(B/Q)=\{\,\sigma_1\,,\sigma_2\,,\cdots\cdots\cdots,\sigma_n\}$ とすると、M の元 η で $(\sigma_1(\eta)\,,\sigma_2(\eta)\,,\cdots\cdots\cdots,\sigma_n(\eta)\,)$が$Q$上の基底（生成系であって 1 次独立）となるものがある。つまり、

$M=\{a_1\,\sigma_1(\eta)+\ a_2\sigma_2(\eta)+\cdots\cdots\cdots+a_n\sigma_n(\eta)\ \mid\ a_i\in Q\}$

このとき、$(\sigma_1(\eta)\,,\sigma_2(\eta)\,,\cdots\cdots\cdots,\sigma_n(\eta)\,)$を M の Q 上の正規底という。

たとえば、$M=Q(\sqrt{2})$としたとき、M の Q 上の正規底は、

$1+\sqrt{2}$ と $1-\sqrt{2}$ である。

実際、$G(M/Q)=\{\,\sigma_1\,,\sigma_2\ \}$ において

（ただし、$\sigma_1:\sqrt{2}\to\sqrt{2}$,σ_2 ： $\sqrt{2}\to-\sqrt{2}$ ）

M の元 $\eta=1+\sqrt{2}$ は、$\sigma_1(\eta)=1+\sqrt{2}$, $\sigma_2(\eta)=1-\sqrt{2}$

これらは、Q 上の基底である。

$\because\quad a(1+\sqrt{2})+b(1-\sqrt{2})=0\ \Leftrightarrow\ a=b=0$

また、$\{a(1+\sqrt{2}+b(1-\sqrt{2})\ \mid a\ ,b\in Q\}$

$=\{\,a_1+a_2\sqrt{2}\ \mid a_1\,,a_2\in Q\}$

$=Q(\sqrt{2})$ (終)

一般に、

$5k+1=p$ (素数)となる$(k=1,2,\ldots.)$ように、p を選んだとき、

1 の原始 p 乗根を ζ とすれば、$L=Q(\zeta)$ の Q 上ガロア群 G は

位数 $p-1\ (=5k)$ の巡回群である。

そして、位数 k の G の部分群 Hに

対応する Lと Qの中間体Mは、Qの

5 次の巡回拡大である。

$$\left.\begin{array}{ccc} L & \ldots & \{i\} \\ k| & & k| \\ M & \ldots & H \\ 5| & & 5| \\ Q & \ldots & G \end{array}\right\} 5k=p-1$$

$M=Q(\eta)$とすれば、$(M/Q)=5$

であるから、η のQ上 5 次の最小

多項式が得られる。

$p=31\ \ (k=6)$としたものが、上記のもので、

ほかに、$p=11\ \ (k=2)$とすれば、

$f(x)=x^5+x^4-4x^3-3x^2+3x+1\ \ (=0)$ が得られる。

ほかに、$p=41\ \ (k=8)$とすれば、

$f(x)=x^5+x^4-16x^3+5x^2+21x-9\ \ (=0)$ が得られる。

Q 上既約な 5 次方程式 $f(x)=0$ が、ガロア群 D_{10} ,(F_{20}) を持つ場合
$f(x)=0$ の 1 つの解を α としたとき、$Q(\omega_p,\omega_5)(\alpha)$ が$Q(\omega_p,\omega_5)$
の巡回拡大となるような、素数 $p=2t+1$,$(p=4t+1)$ が存在する。
(ただし、ω_p,ω_5は、それぞれ 1 の原始 p , 5 乗根を意味する)

② F_{20} をガロア群にもつ、

$f(x)=x^5-20x^3-60x^2-70x-30=0$ の解

($f(x)\equiv x^5\ \ (mod\ \ 5)$ となることを踏まえて)

$f(x)=0$ の 1 つの解を α とし、

$f(x)$ の分解体を L 、

γ を$(Q(\gamma)/Q)=4$ を満たすものとする。

$f(x)\equiv x^5\ \ \ (mod\ \ 5)$ となることから

$Q(\gamma)\subseteq Q(\omega_5)$ であり、$Q(\gamma)=Q(\omega_5)$

$$20\left[\begin{array}{ccc} L=Q(\gamma,\alpha) & \cdots & \{\,i\,\} \\ 5| & & | \\ M{=}Q(\gamma) & \cdots & C_5 \\ 4| & & | \\ Q & \cdots & F_{20} \end{array}\right.$$

(ただし、ω_5 は、1 の原始 5 乗根)

これより、

$L=Q(\omega_5,\alpha)$ となって L は $M=Q(\omega_5)$ の巡回拡大

L の M上のガロア群は巡回群。

$f(x)=0$ の解を $\alpha=\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5$ とし、

$u(\alpha,1)=\alpha_1+\omega_5\alpha_2+{\omega_5}^2\alpha_3+{\omega_5}^3\alpha_4+{\omega_5}^4\alpha_5$

$u(\alpha,2)=\alpha_1+{\omega_5}^2\alpha_2+{\omega_5}^4\alpha_3+\omega_5\alpha_4+{\omega_5}^3\alpha_5$

$u(\alpha,3)=\alpha_1+{\omega_5}^3\alpha_2+\omega_5\alpha_3+{\omega_5}^4\alpha_4+{\omega_5}^2\alpha_5$

$u(\alpha,4)=\alpha_1+{\omega_5}^4\alpha_2+{\omega_5}^3\alpha_3+{\omega_5}^2\alpha_4+\omega_5\alpha_5$

$u(\alpha,5)=\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5 \quad (=0)$ とおくと、

$u(\alpha,k)^5\in M \quad (k=1,2,\dots,5)$

$u(\alpha,1)u(\alpha,4)\in M \quad ,u(\alpha,2)u(\alpha,3)\in M$ などが得られ、

$u(\alpha,1)=5(\sqrt[5]{2})^2\omega_5$

$u(\alpha,2)=5(\sqrt[5]{2})^4{\omega_5}^2$

$u(\alpha,3)=5(\sqrt[5]{2})^1{\omega_5}^3$

$u(\alpha,4)=5(\sqrt[5]{2})^3{\omega_5}^4$ 　　と求まる。

これによって

$$\alpha_1=\frac{u(\alpha,1)+u(\alpha,2)+u(\alpha,3)+u(\alpha,4)+u(\alpha,5)}{5}$$

$$=\left(\sqrt[5]{2}\right)^2\omega_5+\left(\sqrt[5]{2}\right)^4{\omega_5}^2+\left(\sqrt[5]{2}\right)^1{\omega_5}^3+\left(\sqrt[5]{2}\right)^3{\omega_5}^4$$

他の解は、

$\alpha_2=(\sqrt[5]{2})^1\omega_5+(\sqrt[5]{2})^2{\omega_5}^2+(\sqrt[5]{2})^3{\omega_5}^3+(\sqrt[5]{2})^4{\omega_5}^4$

$\alpha_3=(\sqrt[5]{2})^4\omega_5+(\sqrt[5]{2})^3{\omega_5}^2+(\sqrt[5]{2})^2{\omega_5}^3+(\sqrt[5]{2})^1{\omega_5}^4$

$\alpha_4=(\sqrt[5]{2})^3\omega_5+(\sqrt[5]{2})^1{\omega_5}^2+(\sqrt[5]{2})^4{\omega_5}^3+(\sqrt[5]{2})^2{\omega_5}^4$

$\alpha_5=(\sqrt[5]{2})^1 \quad +(\sqrt[5]{2})^2 \quad +(\sqrt[5]{2})^3 \quad +(\sqrt[5]{2})^4$

2 ルンゲの定理

C.Runge (1856-1927)の「Uber die auflosbaren Gleichungen

von der $Form\ x^5+ux+v=0$,1885」によると、

『 λ ,μ を有理数とするとき、

$x^5+\frac{5\mu^4(4\lambda+3)}{\lambda^2+1}x+\frac{4\mu^5(2\lambda+1)(4\lambda+3)}{\lambda^2+1}=0$ は代数的に解ける 』

(概要)

λ ,μ を与え、

$u=\frac{5\mu^4(4\lambda+3)}{\lambda^2+1}$,$v=\frac{4\mu^5(2\lambda+1)(4\lambda+3)}{\lambda^2+1}$ とおくと

与式は、$x^5+ux+v=0$ となる。

ここで、

$l=\frac{5\mu^4(4\lambda+3)^2}{\lambda^2+1}$ とすると

$(l-u)^4(l^2-6ul+25u^2)=5^5v^4l$ が成り立つ。

(代入して確かめるとよい)

そして、$l=\frac{z^2}{4}$ で置き換えると

$(z^2-4u)^4(z^4-24uz^2+400u^2)=4^5 5^5v^4z^2$

さらに、$D=4^4u^5+5^5v^4$ で置き換えると

$(z^6-20uz^4+240u^2z^2+320u^3)^2=4^5z^2D$

$\therefore\quad z^6-20uz^4+240u^2z^2+320u^3=\pm 32z\sqrt{D}$

この方程式の6根(z_1,z_2,z_3,z_4,z_5,z_6)は、

$x^5+ux+v=0$ の5根を $\alpha_0,\alpha_1,\alpha_2,\alpha_3,\alpha_4$ とし、

$n_1=\alpha_0\alpha_1+\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_4+\alpha_4\alpha_0$

$n_2=\alpha_0\alpha_2+\alpha_2\alpha_1+\alpha_1\alpha_4+\alpha_4\alpha_3+\alpha_3\alpha_0$

$n_3=\alpha_1\alpha_2+\alpha_2\alpha_4+\alpha_4\alpha_0+\alpha_0\alpha_3+\alpha_3\alpha_1$

$n_4=\alpha_2\alpha_0+\alpha_0\alpha_4+\alpha_4\alpha_1+\alpha_1\alpha_3+\alpha_3\alpha_2$

$n_5=\alpha_3\alpha_2+\alpha_2\alpha_4+\alpha_4\alpha_1+\alpha_1\alpha_0+\alpha_0\alpha_3$

$n_6=\alpha_4\alpha_2+\alpha_2\alpha_0+\alpha_0\alpha_1+\alpha_1\alpha_3+\alpha_3\alpha_4$

$m_1=\alpha_0\alpha_2+\alpha_0\alpha_3+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_4$

$m_2=\alpha_0\alpha_1+\alpha_0\alpha_4+\alpha_1\alpha_3+\alpha_2\alpha_3+\alpha_2\alpha_4$

$m_3=\alpha_0\alpha_1+\alpha_0\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_4+\alpha_1\alpha_4$

$m_4=\alpha_0\alpha_1+\alpha_0\alpha_3+\alpha_1\alpha_2+\alpha_2\alpha_4+\alpha_3\alpha_4$

$m_5=\alpha_0\alpha_2+\alpha_0\alpha_4+\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_3\alpha_4$

$m_6 = \alpha_0\alpha_3 + \alpha_0\alpha_4 + \alpha_1\alpha_2 + \alpha_1\alpha_4 + \alpha_2\alpha_3$

としたとき、

$z_1 = n_1 - m_1 \quad , z_2 = n_2 - m_2 \quad , \cdots\cdots\cdots , z_6 = n_6 - m_6$

で表される。

$z = 2\sqrt{l} \quad \left(または - 2\sqrt{l} \right)$ は、この内の 1 つであるから

いま仮に、$z = 2\sqrt{l} = z_1$ と考えれば

$$
\begin{aligned}
n_1 + m_1 = \ & n_2 + m_2 \\
= & \cdots\cdots\cdots \\
= & n_6 + m_6 \\
= & \ \alpha_0\alpha_1 + \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_0 \\
& \quad + \alpha_0\alpha_2 + \alpha_0\alpha_3 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 \\
= & \ 0
\end{aligned}
$$

(解と係数との関係)　と

$z_1 = n_1 - m_1$ 　とにより、

$z_1 = 2n_1 = 2\sqrt{l}$

$\therefore \ n_1 = \sqrt{l} \ (= -m_1)$

$\therefore \quad \alpha_0\alpha_1 + \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_0$

$= -(\ \alpha_0\alpha_2 + \alpha_0\alpha_3 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 \ )$

$$= \frac{\sqrt{5}\mu^2(4\lambda+3)}{\sqrt{\lambda^2+1}}$$

これと、解(根)と係数との関係、

$\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$

$\alpha_0\alpha_1 + \alpha_0\alpha_2 + \cdots\cdots\cdots\cdots\cdots + \alpha_3\alpha_4 = 0$

$\alpha_0\alpha_1\alpha_2 + \alpha_0\alpha_1\alpha_3 + \cdots\cdots\cdots\cdots + \alpha_2\alpha_3\alpha_4 = 0$

$\alpha_0\alpha_1\alpha_2\alpha_3 + \alpha_0\alpha_1\alpha_2\alpha_4 + \cdots\cdots\cdots + \alpha_1\alpha_2\alpha_3\alpha_4 \quad = u$

$\alpha_0\alpha_1\alpha_2\alpha_3\alpha_4 \ = -v$

を併用すると、$\alpha_0 , \alpha_1 , \alpha_2 , \alpha_3 , \alpha_4$ が求まるはず。　(終)

なお、『　$\lambda \ , \mu$ を有理数とするとき、

$x^5 + \frac{5\mu^4(4\lambda+3)}{\lambda^2+1} x + \frac{4\mu^5(2\lambda+1)(4\lambda+3)}{\lambda^2+1} = 0$ は、F_{20} 内にガロア群をもつ　』

が示されている。

たとえば、

①　$\mu = 1 \ , \lambda = 4/3$ のとき、

$x^5+15x+44=0$ が得られるがこの方程式のガロア群は
F_{20} に同型であって、代数的に可解である。

② $\mu=1$,$\lambda=1/2$ のとき、
$x^5+20x+32=0$ が得られるがこの方程式のガロア群は
D_{10} に同型であって、代数的に可解である。

なお、ルンゲが示した式と似ているが
1944 年、Spearman と Williams によって
『 c ,e を有理数、$\varepsilon=\pm1$ とするとき

$$x^5+\frac{5e^4(3-4\epsilon c)}{c^2+1}x-\frac{4e^5(11\epsilon+2c)}{c^2+1}=0$$ は

代数的に解ける 』 が証明されている。

③ エルミートの解法

楕円積分　$u=\int_0^x \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$ の逆関数を $x=sn(u,k)$ 、

あるいは、単に $x=sn\,u$ で表す。(k を母数という)

また、$K=\int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}=\int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-k^2sin^2\theta}}$

$L=\int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-l^2t^2)}}=\int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-l^2sin^2\theta}}$

(ただし、$k^2+l^2=1$ で、l を補母数という)

とおくと、

$sn(u+4K)=sn\,u$　,$sn(u+2iL)=sn\,u$ となり、

$\alpha=4K$,$\alpha'=2iL$ は基本周期とよばれる。

k ,l より、K ,L が求まるが、逆に、比 L/K により k ,l も定まる。

すなわち、i の文字は虚数単位を表すとして

$\omega=\frac{iL}{K}$　,$q=e^{i\pi\omega}=e^{\frac{-\pi L}{K}}$　とすれば

$$\sqrt[4]{k}=\sqrt{2}\sqrt[8]{q}\sum_{m=-\infty}^{m=\infty}\frac{q^{2m^2+m}}{q^{m^2}}$$

$$=\sqrt{2}\sqrt[8]{q}\ \frac{1+q+q^3+q^6+q^{10}+q^{15}+q^{21}+q^{28}+q^{36}+\cdots\cdots\cdots}{1+2q+2q^4+2q^9+2q^{16}+2q^{25}+2q^{36}+\cdots\cdots\cdots}$$

が得られ、これらは、ω の関数とも思えるから

$\sqrt[4]{k}=\phi(\omega)$ とおける。

一方、$Jacobi\left(独\,1804-1851\right)$ によって得られた楕円積分の

変換原理によれば、

『 任意の奇数 n , 任意の数 k に対し、$y=\frac{U(x)\quad\cdots\cdots\cdots n次奇多項式}{V(x)\quad\cdots\cdots n-1\ 次偶多項式}$ と

するとき、 $\frac{dy}{\sqrt{(1-y^2)(1-l^2y^2)}}=M\cdot\frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$　が成立する

ような定数 l ,M が存在する 』

実際、$n=3$　の場合、

$y=\frac{(v+2u^3)vx+u^6x^3}{v^2+u^3(2v+u^3)x^2}$ とすれば、

$\frac{dy}{\sqrt{(1-y^2)(1-l^2y^2)}} = \frac{u+2u^3}{v} \cdot \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$　が成り立つ

ただし、$u = \sqrt[4]{k}$　, $v = \sqrt[4]{l}$ であり、u と v の間には

$u^4 - v^4 + 2uv(1 - u^2v^2) = 0$ の関係式が成り立つ
(この母数 k , l の変換前後の関係式をモジュラー方程式という)

$n = 5$ の場合のモジュラー方程式は、
$u^6 - v^6 + 5u^2v^2(u^2 - v^2) + 4uv(1 - u^4v^4) = 0$
で与えられ、$u = \sqrt[4]{k} = \phi(\omega)$ とし、v についての式
$v^6 + 4u^5v^5 + 5u^2v^4 - 5u^4v^2 - 4uv - u^6 = 0$
とみたとき、その 6 根は、

$v_0 = -\phi(5\omega)$　, $v_{m+1} = \phi\left(\frac{\omega+16m}{5}\right)$　$(m = 0,1,2,3,4)$

で表される。

v_0 は、$\sqrt[4]{k} = \phi(\omega) = \sqrt{2}\,\sqrt[8]{q}\,\sum_{m=-\infty}^{m=\infty} \frac{q^{2m^2+m}}{q^{m^2}}$

$$= \sqrt{2}\,\sqrt[8]{q}\,\frac{1 + q + q^3 + q^6 + q^{10} + q^{15} + q^{21} + q^{28} + q^{36} + \cdots\cdots\cdots}{1 + 2q + 2q^4 + 2q^9 + 2q^{16} + 2q^{25} + 2q^{36} + \cdots\cdots\cdots}$$

の式において

$q = e^{i\pi\omega} = e^{\frac{-\pi L}{K}}$ なので、q の代わりに q^5 を代入し符号を

変えたものだし、v_{m+1} $(m = 0,1,2,3,4)$ は、q の代わりに

$q^{\frac{1}{5}} \cdot \left(e^{\frac{16\pi i}{5}}\right)^m = q^{\frac{1}{5}} \cdot \left(e^{\frac{6\pi i}{5}}\right)^m$　$(m = 0,1,2,3,4)$ を代入したものである。

いま、
$\Phi_0(\omega) = (v_1 - v_0)(v_2 - v_5)(v_3 - v_4)$
$\Phi_1(\omega) = (v_2 - v_0)(v_3 - v_1)(v_4 - v_5)$
$\Phi_2(\omega) = (v_3 - v_0)(v_4 - v_2)(v_5 - v_1)$
$\Phi_3(\omega) = (v_4 - v_0)(v_5 - v_3)(v_1 - v_2)$
$\Phi_4(\omega) = (v_5 - v_0)(v_1 - v_4)(v_2 - v_3)$
とおき、
$(y - \Phi_0(\omega))(y - \Phi_1(\omega))(y - \Phi_2(\omega))(y - \Phi_3(\omega))(y - \Phi_4(\omega)) = 0$
を作ると、これは、5 次方程式、
$y^5 - 2000u^4(1 - u^8)^2 y$

$-1600\sqrt{5}\,u^3\left(1-u^8\right)^2(1+u^8)=0$ を満たす。

さらに、

$y=\sqrt[4]{2000}\,u\sqrt{1-u^8}\cdot x$ とおくと、

$x^5-x-\frac{2\left(1+u^8\right)}{\sqrt[4]{5^5}\,u^2\sqrt{1-u^8}}=0$

これにより、$x^5-x-a=0$ の形の５次方程式を解くには

（一般の５次方程式は、理論的には、チルンハウス変換などによって

この形に変形できるので、これだけ解ければ十分である。）

$\frac{2\left(1+u^8\right)}{\sqrt[4]{5^5}\,u^2\sqrt{1-u^8}}=a$ とし、$A=\sqrt[4]{5^5}\,a\,/2$ とおくと、

$u=\sqrt[4]{k}$ より $u^2=\sqrt{k}$, $u^8=k^2$ で

$k^4+A^2k^3+2k^2-A^2k+1=0$ が得られる。

これは、

$(k-k^{-1})^2+A^2(k-k^{-1})+4=0$ と変形でき、

$k-k^{-1}=\left(-A^2\pm\sqrt{A^4-16}\right)/\,2$ から、k の値が求まる。

そして、これより、$\sqrt[4]{k}=\phi(\omega)$ が決まり

$v_0=-\phi(5\omega)$, $v_{m+1}=\phi\left(\frac{\omega+16m}{5}\right)$ $(m=0,1,2,3,4)$

を求めれば、（ここが代数的ではない）

$\Phi_0(\omega)$, $\Phi_1(\omega)$, $\Phi_2(\omega)$, $\Phi_3(\omega)$, $\Phi_4(\omega)$ が求まる。

そのとき、

$x=\frac{y}{\sqrt[4]{2000}\,u\sqrt{1-u^8}}=\frac{\Phi_m(\omega)}{\sqrt[4]{2000}\,\sqrt[4]{k}\sqrt{1-k^2}}$ $(m=0,1,2,3,4)$ が

$x^5-x-a=0$ の解である。

【例】 エルミートの解法によって、S_5 をガロア群にもつ
$x^5-80x+192=0$ の解（近似値）を求めてみる
ただし、コンピューターの助けが必要である

（解法）

$x=\sqrt[4]{80}\,y$ とおくと、

$y^5-y+\frac{6}{(\sqrt[4]{5})^5}=0$

ここで、$\frac{6}{(\sqrt[4]{5})^5}=-a$ と考えると、

$A=\frac{(\sqrt[4]{5})^5 a}{2}=\frac{(\sqrt[4]{5})^5}{2}\cdot\frac{-6}{(\sqrt[4]{5})^5}=-3 \qquad (\therefore A^2=9)$

これより、

$k^4+9k^3+2k^2-9k+1=0$ を解いて、その 1 つを

$k=(-9+\sqrt{65}+3\sqrt{18-2\sqrt{65}}\,)/4$

$=0.792676910548$

$k^2=0.628336684515$

$\therefore\quad l^2=1-k^2=0.371663315485$

これより、

$$K=\int_0^{\frac{\pi}{2}}\frac{d\theta}{\sqrt{1-k^2sin^2\theta}}=1.98142022191$$

$L=\int_0^{\frac{\pi}{2}}\frac{d\theta}{\sqrt{1-l^2sin^2\theta}}$=1.7583631759

$\pi=3.14159265359$

$q=e^{\left(-\frac{\pi L}{K}\right)}=0.06154848886\ldots..$

よって、

$q_1=q^5=0.000000883256766$

$q_2=q^{\frac{1}{5}}=0.57258963071$

ここで、$t=e^{\frac{6\pi i}{5}}=-0.80901699437-0.58778525229\cdot i$ とし、

$$q_3=t\cdot q^{\frac{1}{5}}=-0.46323474205-0.33655974055\,i$$

$$q_4=t^2\cdot q^{\frac{1}{5}}=0.17693992669+0.54456509945\,i$$

$$q_5=t^3\cdot q^{\frac{1}{5}}=0.17693992669-0.54456509945\,i$$

$$q_6 = t^4 \cdot q^{\frac{1}{5}} = -0.4632347420 + 0.33655974055\, i$$

ここで、

$$f(x) = \sqrt{2}\ \sqrt[8]{q}\ \frac{1+q+q^3+q^6+q^{10}+q^{15}+q^{21}+q^{28}+q^{36}+\cdots\cdots}{1+2q+2q^4+2q^9+2q^{16}+2q^{25}+2q^{36}+\cdots\cdots}$$ 、

$\sqrt{2} = 1.41421356237$ とし、$f(x)$ の x の値に q_1 を代入し符号を変えたものを v_0 , q_2 から q_6 を代入したものを v_1 ,……, v_5 とすれば、

$v_0 = -0.24761416533$

$v_1 = 0.9999999589$

$v_2 = -1.216395910 + 1.426726636\, i$

$v_3 = -0.655689043 + 0.617161841\, i$

$v_4 = -0.655689043 - 0.617161841\, i$

$v_5 = -1.216395910 - 1.426726636\, i$

〘ここで注意：

v_2 の計算の中では、$\sqrt[8]{q_3}$ の代わりに $\sqrt[8]{q_3}\cdot i$ を用いている

v_3 の計算の中では、$\sqrt[8]{q_4}$ の代わりに $\sqrt[8]{q_4}\cdot(-\sqrt{-i}\,)$ を用いている

v_4 の計算の中では、$\sqrt[8]{q_5}$ の代わりに $\sqrt[8]{q_5}\cdot(-\sqrt{i}\,)$ を用いている

v_5 の計算の中では、$\sqrt[8]{q_6}$ の代わりに $\sqrt[8]{q_6}\cdot(-i\,)$ を用いている 〙

これらと $x = \sqrt[4]{80}\, y$, $k = 0.792676910548$ とにより、

$$x_1 = \sqrt[4]{80}\, y_1 = \sqrt[4]{80}\cdot\frac{(v_1-v_0)(v_2-v_5)(v_3-v_4)}{\sqrt[4]{2000}\sqrt[4]{k}\sqrt{1-k^2}} = -3.41622296$$

$$x_2 = \sqrt[4]{80}\, y_2 = \sqrt[4]{80}\cdot\frac{(v_2-v_0)(v_3-v_1)(v_4-v_5)}{\sqrt[4]{2000}\sqrt[4]{k}\sqrt{1-k^2}} = 2.17843088 - 0.83500826\, i$$

$$x_3 = \sqrt[4]{80}\, y_3 = \sqrt[4]{80}\cdot\frac{(v_3-v_0)(v_4-v_2)(v_5-v_1)}{\sqrt[4]{2000}\sqrt[4]{k}\sqrt{1-k^2}} = -0.47031941 - 3.17880674\, i$$

$$x_4 = \sqrt[4]{80}\, y_4 = \sqrt[4]{80}\cdot\frac{(v_4-v_0)(v_5-v_3)(v_1-v_2)}{\sqrt[4]{2000}\sqrt[4]{k}\sqrt{1-k^2}} = -0.47031941 + 3.17880674\, i$$

$$x_5 = \sqrt[4]{80}\, y_5 = \sqrt[4]{80}\cdot\frac{(v_5-v_0)(v_1-v_4)(v_2-v_3)}{\sqrt[4]{2000}\sqrt[4]{k}\sqrt{1-k^2}} = 2.17843088 + 0.83500826\, i$$

4 代数的解法

5 次方程式の x^4 の項は簡単に消去できるので

$x^5+a_3x^3+a_2x^2+a_1x+a_0$ ……………………(1)

の形のものを考える。(1)の解を x_1 ,x_2 ,x_3 ,x_4 ,x_5 とし

ζ を 1 の原始 5 乗根とする。($\zeta^5=1,\zeta\neq 1,\ \zeta^4+\zeta^3+\zeta^2+\zeta^1+1=0$)

$$\left.\begin{aligned}x_1&=p+q+r+s\\x_2&=p\zeta^1+q\zeta^2+r\zeta^3+s\zeta^4\\x_3&=p\zeta^2+q\zeta^4+r\zeta^1+s\zeta^3\\x_4&=p\zeta^3+q\zeta^1+r\zeta^4+s\zeta^2\\x_5&=p\zeta^4+q\zeta^3+r\zeta^2+s\zeta^1\end{aligned}\right\}\cdots\cdots\cdots\cdots(2)$$ とおくと

$(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)=0$ を展開した式と

(1) の式の係数を比べて、(解と係数との関係)

$x_1+x_2+x_3+x_4+x_5=0$ ……………………(3)

$x_1x_2+x_1x_3+x_1x_4+x_1x_5+x_2x_3+x_2x_4+x_2x_5+x_3x_4+x_3x_5+x_4x_5$

$=-5(ps+qr)=a_3$ ……………………………………………(4)

$x_1x_2x_3+x_1x_2x_4+x_1x_2x_5+x_1x_3x_4+x_1x_3x_5+x_1x_4x_5+x_2x_3x_4+x_2x_3x_5+x_2x_4x_5+x_3x_4x_5$

$=5(p^2r+pq^2+qs^2+r^2s)=-a_2$ ……………………………(5)

$x_1x_2x_3x_4+x_1x_2x_3x_5+x_1x_2x_4x_5+x_1x_3x_4x_5+x_2x_3x_4x_5$

$=-5(p^3q-q^2r^2+pr^3+q^3s+pqrs-p^2s^2+rs^3)=a_1$ …………(6)

$x_1x_2x_3x_4x_5$

$=(p^5+q^5+r^5+s^5)-5(ps-qr)(p^2r-pq^2+qs^2-r^2s)=-a_0$ …(7)

p ,q ,r ,s を求めるには、(3)～(6)の連立方程式を解けばよいが、
一般の 5 次方程式は代数的に解けないのでこの連立方程式も解けない。
ところが、代数的に解ける場合は、

$\{25(ps-qr)\}^2=$ 有理数 $\left(=\alpha\right.$ とする$\left.\right)$ ……………………(8)

$\{125(p^2r-pq^2+qs^2-r^2s)\}^2=$ 有理数 ($=\beta$ とする) ………… (9)

となることがわかっていて、これらを追加することで p ,q ,r ,s が
求まり、最終的な解 x_1 ,x_2 ,x_3 ,x_4 ,x_5 が求まるというもの。

<そのために、まず α ,β の値を求める>

(2)の式を p, q, r, s について解くと

$$\left.\begin{aligned}
p &= (x_1 + \zeta^4 x_2 + \zeta^3 x_3 + \zeta^2 x_4 + \zeta^1 x_5)/5 \\
q &= (x_1 + \zeta^3 x_2 + \zeta^1 x_3 + \zeta^4 x_4 + \zeta^2 x_5)/5 \\
r &= (x_1 + \zeta^2 x_2 + \zeta^4 x_3 + \zeta^1 x_4 + \zeta^3 x_5)/5 \\
s &= (x_1 + \zeta^1 x_2 + \zeta^2 x_3 + \zeta^3 x_4 + \zeta^4 x_5)/5
\end{aligned}\right\} \cdots\cdots\cdots\cdots (10)$$

これらの式を(8)の左辺の式に代入すると、α が x_1, x_2, x_3, x_4, x_5 の多項式で表される。これを $\alpha(x_1, x_2, x_3, x_4, x_5)$ と表すことにするがこれは、x_1, x_2, x_3, x_4, x_5 の対称式ではない。

そこで、この式の x_1, x_2, x_3, x_4, x_5 に 5!=120 通りの置換を作用させるとすべて異なる式になるのではなく、$\alpha(x_1, x_2, x_3, x_4, x_5)$ と同じものが 20 個、$\alpha(x_1, x_2, x_3, x_5, x_4)$ と同じものが 20 個、$\alpha(x_1, x_2, x_4, x_3, x_5)$ と同じものが 20 個、$\alpha(x_1, x_2, x_4, x_5, x_3)$ と同じものが 20 個、$\alpha(x_1, x_2, x_5, x_3, x_4)$ と同じものが 20 個、$\alpha(x_1, x_2, x_5, x_4, x_3)$ と同じものが 20 個となる。

ここで、

$$\begin{aligned}
f_\alpha(x) = &(x - \alpha(x_1, x_2, x_3, x_4, x_5))(x - \alpha(x_1, x_2, x_3, x_5, x_4)) \\
&\times (x - \alpha(x_1, x_2, x_4, x_3, x_5))(x - \alpha(x_1, x_2, x_4, x_5, x_3)) \\
&\times (x - \alpha(x_1, x_2, x_5, x_3, x_4))(x - \alpha(x_1, x_2, x_5, x_4, x_3))
\end{aligned}$$

を作ると、これは、x_1, x_2, x_3, x_4, x_5 の対称式であり、その係数は a_3, a_2, a_1, a_0 で表される。

しかも当然ながら、$f_\alpha(x) = 0$ の解の 1 つは、α である。

(一見すると、解を求めるのに次数が 1 つ上がった 6 次方程式を考えるので矛盾するように思えるが因数分解できるので、α が求まる)

ちなみに、コンピューターを利用すると、

$$\begin{aligned}
f_\alpha(x) = &x^6 + (-200a_1 - 30{a_3}^2)x^5 \\
&+ \begin{pmatrix} 22000{a_1}^2 - 20000a_0a_2 + 800{a_2}^2a_3 \\ +2600a_1{a_3}^2 + 375{a_3}^4 \end{pmatrix} x^4 \\
&+ \cdots\cdots\cdots\cdots \text{ (長い式になる)}
\end{aligned}$$

同じように、

(10)の式を(9)の左辺の式に代入すると、β が x_1, x_2, x_3, x_4, x_5 の多項式で表される。これを $\beta(x_1, x_2, x_3, x_4, x_5)$ と表すことにし、

$$\begin{aligned}
f_\beta(x) = &(x - \beta(x_1, x_2, x_3, x_4, x_5))(x - \beta(x_1, x_2, x_3, x_5, x_4)) \\
&\times (x - \beta(x_1, x_2, x_4, x_3, x_5))(x - \beta(x_1, x_2, x_4, x_5, x_3)) \\
&\times (x - \beta(x_1, x_2, x_5, x_3, x_4))(x - \beta(x_1, x_2, x_5, x_4, x_3))
\end{aligned}$$

を考えると

$$
\begin{aligned}
f_\beta(x) = x^6 &+ (-750{a_2}^2 + 2000a_1a_3)x^5 \\
&+ \begin{pmatrix} -2000000{a_1}^3 + 7500000a_0a_1a_2 + 234375{a_2}^4 \\ -12500000{a_0}^2a_3 - 1250000a_1{a_2}^2a_3 \\ +1500000{a_1}^2{a_3}^2 + 500000a_0a_2{a_3}^2 \end{pmatrix} x^4
\end{aligned}
$$

$+\cdots\cdots\cdots\cdots\cdots$　　　（かなり長い式になる）

当然、 $f_\beta(x) = 0$ の解の１つは、β である。

＜このあと、上記で得られる α ，β の値と(4)(5)(8)(9)の式を
用いて、 $p\,,q\,,r\,,s$ を求める。 (6)(7)は検算に使う＞

再度書くと、

$$
\begin{cases}
(ps + qr) = -a_3/5 & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (4) \\
(p^2r + pq^2 + qs^2 + r^2s) = -a_2/5 & \cdots\cdots\cdots (5) \\
(ps - qr) = \pm\sqrt{\alpha}\,/25 & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (8) \\
(p^2r - pq^2 + qs^2 - r^2s) = \pm\sqrt{\beta}\,/125 & \cdots\cdots (9)
\end{cases}
$$

(4)(8)より、

$$ps = (-5a_3 \pm \sqrt{\alpha}\,)/50 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (10)$$

$$qr = (-5a_3 \mp \sqrt{\alpha}\,)/50 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (11)$$

（複号は同順）

(5)(9)より、

$$p^2r + qs^2 = (-25a_2 \pm \sqrt{\beta}\,)/250 \quad \cdots\cdots\cdots\cdots (12)$$

$$pq^2 + r^2s = (-25a_2 \mp \sqrt{\beta}\,)/250 \quad \cdots\cdots\cdots\cdots (13)$$

（複号は同順）

また、

$$(p^2r)(qs^2) = (ps)^2(qr) = \left(-5a_3 \pm \sqrt{\alpha}\,\right)^2(-5a_3 \mp \sqrt{\alpha}\,)/125000 \quad \cdots (14)$$

$$(pq^2)(r^2s) = (ps)(qr)^2 = (-5a_3 \pm \sqrt{\alpha}\,)\left(-5a_3 \mp \sqrt{\alpha}\,\right)^2/125000 \quad \cdots (15)$$

(複号は同順)

(12)(14)より、p^2r と qs^2 は、

$$t^2 - \left(\frac{-25a_2 \pm \sqrt{\beta}}{250}\right)t + \frac{\left(-5a_3 \pm \sqrt{\alpha}\right)^2\left(-5a_3 \mp \sqrt{\alpha}\right)}{125000} = 0$$

の２解であり、

$$p^2r = \frac{\left(\dfrac{-25a_2 \pm \sqrt{\beta}}{250}\right) - \sqrt{\left(\dfrac{-25a_2 \pm \sqrt{\beta}}{250}\right)^2 - \dfrac{4\left(-5a_3 \pm \sqrt{\alpha}\right)^2\left(-5a_3 \mp \sqrt{\alpha}\right)}{125000}}}{2} \quad \cdots (16)$$

$$qs^2 = \frac{\left(\frac{-25a_2 \pm \sqrt{\beta}}{250}\right) + \sqrt{\left(\frac{-25a_2 \pm \sqrt{\beta}}{250}\right)^2 - \frac{4\left(-5a_3 \pm \sqrt{\alpha}\right)^2\left(-5a_3 \mp \sqrt{\alpha}\right)}{125000}}}{2} \quad \cdots(17)$$

（ただし、第１項の複号と第２項の複号は、同順とは限らない）

また、(13)(15)より、pq^2 とr^2s は、

$$t^2 - \left(\frac{-25a_2 \mp \sqrt{\beta}}{250}\right)t + \frac{\left(-5a_3 \pm \sqrt{\alpha}\right)\left(-5a_3 \mp \sqrt{\alpha}\right)^2}{125000} = 0$$ の２解であり、

$$pq^2 = \frac{\left(\frac{-25a_2 \mp \sqrt{\beta}}{250}\right) - \sqrt{\left(\frac{-25a_2 \mp \sqrt{\beta}}{250}\right)^2 - \frac{4\left(-5a_3 \pm \sqrt{\alpha}\right)\left(-5a_3 \mp \sqrt{\alpha}\right)^2}{125000}}}{2} \quad \cdots(18)$$

$$r^2s = \frac{\left(\frac{-25a_2 \mp \sqrt{\beta}}{250}\right) + \sqrt{\left(\frac{-25a_2 \mp \sqrt{\beta}}{250}\right)^2 - \frac{4\left(-5a_3 \pm \sqrt{\alpha}\right)\left(-5a_3 \mp \sqrt{\alpha}\right)^2}{125000}}}{2} \quad \cdots(19)$$

（ただし、第１項の複号と第２項の複号は、同順とは限らない）

これで、(11)(16)(18)の値を使えば、

$p^5 = \frac{(p^2r)^2(pq^2)}{(qr)^2}$ より、p^5 が求まり、 p が求まる。

同様に、

$q^5 = \frac{(pq^2)^2(qs^2)}{(ps)^2}$ より、q^5 が求まり、 q が求まる。

$r^5 = \frac{(r^2s)^2(p^2r)}{(ps)^2}$ より、r^5 が求まり、 r が求まる。

$s^5 = \frac{(qs^2)^2(r^2s)}{(qr)^2}$ より、s^5 が求まり、 s が求まる。

こうして、ps と qr , p^2rと qs^2 、pq^2と r^2s 、p^5, q^5, r^5, s^5 が求まったところで、

$$-5(p^3q + pr^3 + q^3s + rs^3 + pqrs - p^2s^2 - q^2r^2)$$

$$= -5\left(\begin{array}{c}\frac{p^2r \cdot pq^2}{qr} + \frac{p^2r \cdot r^2s}{ps} + \frac{pq^2 \cdot qs^2}{ps} + \frac{qs^2 \cdot r^2s}{qr} \\ +(ps)(qr) - (ps)^2 - (qr)^2\end{array}\right) = a_1 \quad \cdots\cdots(6)$$

$$-(p^5 + q^5 + r^5 + s^5) + 5(ps - qr)(p^2r - pq^2 + qs^2 - r^2s) = a_0 \quad \cdots\cdots(7)$$

となるかどうかの確認をしておく。不成立の場合は、適当に式を変え、ps と qr 、p^2rと qs^2 、pq^2と r^2s の値を求め直す。

こうして、p, q, r, s が確定すれば、解として

$x_1 = p + q + r + s$
$x_2 = p\zeta^1 + q\zeta^2 + r\zeta^3 + s\zeta^4$
$x_3 = p\zeta^2 + q\zeta^4 + r\zeta^1 + s\zeta^3$
$x_4 = p\zeta^3 + q\zeta^1 + r\zeta^4 + s\zeta^2$
$x_5 = p\zeta^4 + q\zeta^3 + r\zeta^2 + s\zeta^1$　　　が求まる。　　　　　　（終）

★★ 以下、文字の扱いは前述に従うものとする ★★

(例 1)　　$x^5 - 20x^3 - 60x^2 - 70x - 30 = 0$ の解
（この方程式のガロア群は、F_{20} に同型）

$a_3 = -20$,$a_2 = -60$,$a_1 = -70$,$a_0 = -30$
また、
$f_\alpha(x) = x^6 + 2\cdot 10^3 x^5 + 14\cdot 10^5 x^4 + 4\cdot 10^8 x^3 + 4\cdot 10^{10} x^2 - 16\cdot 10^{10} x$
$= x(x^5 + 2\cdot 10^3 x^4 + 14\cdot 10^5 x^3 + 4\cdot 10^8 x^2 + 4\cdot 10^{10} x - 16\cdot 10^{10})$
∴ $f_\alpha(x) = 0$ から、$x = 0$ が得られ、$\alpha = 0$
$f_\beta(x) = x^6 + 1\cdot 10^5 x^5 + 35\cdot 10^8 x^4 + 5\cdot 10^{13} x^3 + 25\cdot 10^{16} x^2 + (-140625\cdot 10^{16})x$
$= x(x^5 + 1\cdot 10^5 x^4 + 35\cdot 10^8 x^3 + 5\cdot 10^{13} x^2 + 25\cdot 10^{16} x + (-140625\cdot 10^{16}))$
∴ $f_\beta(x) = 0$ から、$x = 0$ が得られ、$\beta = 0$
これより、
$ps = 2$
$qr = 2$
また、p^2r と qs^2 は、
$t^2 - 6t + 8 = 0$ の 2 解で
$p^2r = 2$
$qs^2 = 4$
また、pq^2 とr^2s も
$t^2 - 6t + 8 = 0$ の 2 解で
$pq^2 = 2$
$r^2s = 4$
よって、

$p^5 = \frac{(p^2r)^2(pq^2)}{(qr)^2} = \frac{4\cdot 2}{4} = 2$

$q^5 = \frac{(pq^2)^2(qs^2)}{(ps)^2} = \frac{4\cdot 4}{4} = 4 = 2^2$

$$r^5=\frac{(r^2s)^2(p^2r)}{(ps)^2}=\frac{16\cdot 2}{4}=8=2^3$$

$$s^5=\frac{(qs^2)^2(r^2s)}{(qr)^2}=\frac{16\cdot 4}{4}=16=2^4$$

$$p^3q=\frac{p^2r\cdot pq^2}{qr}=2\qquad ,pr^3=\frac{p^2r\cdot r^2s}{ps}=4\quad ,$$

$$q^3s=\frac{pq^2\cdot qs^2}{ps}=4\qquad ,rs^3=\frac{qs^2\cdot r^2s}{qr}=8$$

これらを使うと (6),(7)式の

$$-5(p^3q+pr^3+q^3s+rs^3+pqrs-p^2s^2-q^2r^2)$$

$$=-5\left(\begin{array}{c}\dfrac{p^2r\cdot pq^2}{qr}+\dfrac{p^2r\cdot r^2s}{ps}+\dfrac{pq^2\cdot qs^2}{ps}+\dfrac{qs^2\cdot r^2s}{qr}\\+(ps)(qr)-(ps)^2-(qr)^2\end{array}\right)=-70=a_1$$

と

$$-(\,p^5+q^5+r^5+s^5)+5(\,ps-qr)(p^2r-pq^2+qs^2-r^2s)=-30=a_0$$

の確認ができる。

これより、

$p=\sqrt[5]{2}\ \ ,q=\sqrt[5]{2^2}\ \ ,r=\sqrt[5]{2^3}\ \ ,s=\sqrt[5]{2^4}$ 　となって

$x^5-20x^3-60x^2-70x-30=0$ の解は、ζ を 1 の原始 5 乗根として

$x_1=p+q+r+s$

$\quad=\sqrt[5]{2}+\sqrt[5]{2^2}+\sqrt[5]{2^3}+\sqrt[5]{2^4}$

$x_2=p\zeta^1+q\zeta^2+r\zeta^3+s\zeta^4$

$\quad=\sqrt[5]{2}\zeta^1+\sqrt[5]{2^2}\zeta^2+\sqrt[5]{2^3}\zeta^3+\sqrt[5]{2^4}\zeta^4$

$x_3=p\zeta^2+q\zeta^4+r\zeta^1+s\zeta^3$

$\quad=\sqrt[5]{2}\zeta^2+\sqrt[5]{2^2}\zeta^4+\sqrt[5]{2^3}\zeta^1+\sqrt[5]{2^4}\,\zeta^3$

$x_4=\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

$x_5=\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$　　　　　　　　　　（終）

(例 2)　$x^5 - x^3 - 2x^2 - 2x - 1 = 0$ の解

（この方程式のガロア群は、D_{10} に同型）

$a_3 = -1$,$a_2 = -2$,$a_1 = -2$,$a_0 = -1$

また、

$$f_\alpha(x) = x^6 + 370x^5 + 39975x^4 + 1001500x^3 -3250625x^2 - 7247768750x + 968765625$$

$$= (x-45)\begin{pmatrix} x^5 + 415x^4 + 58650x^3 + 3640750x^2 \\ +160583125x - 21528125 \end{pmatrix}$$

$\therefore$ $f_\alpha(x) = 0$ から、$x = 45$ が得られ、$\alpha = 45$

$$f_\beta(x) = x^6 + 1000x^5 - 750000x^4 + 5\cdot 10^9 x^3 +3\cdot 10^{12}x^2 + 7178125\cdot 10^{10}x + 75625\cdot 10^{14}$$

$$= (x-2000)\begin{pmatrix} x^5 + 3000x^4 + 525\cdot 10^4 x^3 + 155\cdot 10^8 x^2 \\ +34\cdot 10^{12}x - 378125\cdot 10^{10} \end{pmatrix}$$

$\therefore$ $f_\beta(x) = 0$ から、$x = 2000$ が得られ、$\beta = 2000$

これより、

$ps = (5 - \sqrt{45})/50$

$qr = (5 + \sqrt{45})/50$

また、p^2r と qs^2 を

$$t^2 - \left(\frac{50+\sqrt{2000}}{250}\right)t + \frac{\left(5-\sqrt{45}\right)^2\left(5+\sqrt{45}\right)}{125000} = 0$$ の２解と考えると、

$$t^2 - \left(\frac{5+2\sqrt{5}}{25}\right)t + \frac{\left(-5+3\sqrt{5}\right)}{6250} = 0$$ より

$p^2r = (25 + 10\sqrt{5} - \sqrt{1175 + 470\sqrt{5}})/250$

$qs^2 = (25 + 10\sqrt{5} + \sqrt{1175 + 470\sqrt{5}})/250$

また、pq^2 とr^2s を

$$t^2 - \left(\frac{50-\sqrt{2000}}{250}\right)t + \frac{\left(5-\sqrt{45}\right)\left(5+\sqrt{45}\right)^2}{125000} = 0$$ の２解と考えると、

$$t^2 - \left(\frac{5-2\sqrt{5}}{25}\right)t + \frac{\left(-5-3\sqrt{5}\right)}{6250} = 0$$ より

$pq^2 = (25 - 10\sqrt{5} - \sqrt{1175 - 470\sqrt{5}})/250$

$r^2s = (25 - 10\sqrt{5} + \sqrt{1175 - 470\sqrt{5}})/250$

よって、

$$p^5=\frac{(p^2r)^2(pq^2)}{(qr)^2}$$

$$=-\frac{(-25+10\sqrt{5}+\sqrt{1175-470\sqrt{5}})(-25-10\sqrt{5}+\sqrt{1175+470\sqrt{5}})^2}{6250(5+3\sqrt{5})^2}\quad(\fallingdotseq -3.2383\cdot 10^{-7})$$

$$q^5=\frac{(pq^2)^2(qs^2)}{(ps)^2}=\frac{\left(-25+10\sqrt{5}+\sqrt{1175-470\sqrt{5}}\right)^2(25+10\sqrt{5}+\sqrt{1175+470\sqrt{5}})}{6250(5-3\sqrt{5})^2}\quad(\fallingdotseq 0.374395)$$

$$r^5=\frac{(r^2s)^2(p^2r)}{(ps)^2}=-\frac{\left(25-10\sqrt{5}+\sqrt{1175-470\sqrt{5}}\right)^2(-25-10\sqrt{5}+\sqrt{1175+470\sqrt{5}})}{6250(5-3\sqrt{5})^2}\quad(\fallingdotseq 0.00188049)$$

$$s^5=\frac{(qs^2)^2(r^2s)}{(qr)^2}=\frac{(25-10\sqrt{5}+\sqrt{1175-470\sqrt{5}})(25+10\sqrt{5}+\sqrt{1175+470\sqrt{5}})^2}{6250(5+3\sqrt{5})^2}\quad(\fallingdotseq 0.143725)$$

$$p^3q=\frac{p^2r\cdot pq^2}{qr}\quad,pr^3=\frac{p^2r\cdot r^2s}{ps}\quad,q^3s=\frac{pq^2\cdot qs^2}{ps}\quad,rs^3=\frac{qs^2\cdot r^2s}{qr}$$

これらを使うと (6),(7)式の

$$-5(p^3q+pr^3+q^3s+rs^3+pqrs-p^2s^2-q^2r^2)$$

$$=-5\left(\begin{array}{c}\dfrac{p^2r\cdot pq^2}{qr}+\dfrac{p^2r\cdot r^2s}{ps}+\dfrac{pq^2\cdot qs^2}{ps}+\dfrac{qs^2\cdot r^2s}{qr}\\+(ps)(qr)-(ps)^2-(qr)^2\end{array}\right)=-2=a_1$$

と

$$-(p^5+q^5+r^5+s^5)+5(ps-qr)(p^2r-pq^2+qs^2-r^2s)=-1=a_0$$

の確認ができる。

これより

$$p=\sqrt[5]{-\frac{(-25+10\sqrt{5}+\sqrt{1175-470\sqrt{5}})(-25-10\sqrt{5}+\sqrt{1175+470\sqrt{5}})^2}{6250(5+3\sqrt{5})^2}}\fallingdotseq -0.0503574$$

$$q=\sqrt[5]{\frac{\left(-25+10\sqrt{5}+\sqrt{1175-470\sqrt{5}}\right)^2(25+10\sqrt{5}+\sqrt{1175+470\sqrt{5}})}{6250(5-3\sqrt{5})^2}}\fallingdotseq 0.821611$$

$$r=\sqrt[5]{-\frac{\left(25-10\sqrt{5}+\sqrt{1175-470\sqrt{5}}\right)^2(-25-10\sqrt{5}+\sqrt{1175+470\sqrt{5}})}{6250(5-3\sqrt{5})^2}}\fallingdotseq 0.285006$$

$$s=\sqrt[5]{\frac{(25-10\sqrt{5}+\sqrt{1175-470\sqrt{5}})(25+10\sqrt{5}+\sqrt{1175+470\sqrt{5}})^2}{6250(5+3\sqrt{5})^2}}\fallingdotseq 0.678432$$

となって、

$x^5-x^3-2x^2-2x-1=0$ の解は、ζ を 1 の原始 5 乗根

($\zeta = e^{\frac{2\pi i}{5}} = -\frac{1}{4} + \frac{\sqrt{5}}{4} + i\sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}} \fallingdotseq 0.309017 + 0.951057\,i$)として

$$x_1 = p + q + r + s$$

$$\fallingdotseq -0.0503574 + 0.821611 + 0.285006 + 0.678432 = 1.73469$$

$$x_2 = p\zeta^1 + q\zeta^2 + r\zeta^3 + s\zeta^4$$

$$\fallingdotseq -0.701186 - 0.377712\,i$$

$$x_3 = p\zeta^2 + q\zeta^4 + r\zeta^1 + s\zeta^3$$

$$\fallingdotseq -0.16616 - 0.938713\,i$$

$$x_4 = \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x_5 = \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

（終）

(例 3)　$x^5+15x+44=0$　の解

（この方程式のガロア群は、F_{20} に同型）

$a_3=0$,$a_2=0$,$a_1=15$,$a_0=44$

また、

$$f_\alpha(x)=(x-2500)\begin{pmatrix}x^5-500x^4+37\cdot10^5x^3+547\cdot10^7x^2\\+150925\cdot10^8x-729\cdot10^{10}\end{pmatrix}$$

$\therefore$ $f_\alpha(x)=0$ から、$x=2500$ が得られ、$\alpha=2500$

$$f_\beta(x)==(x-250000)\begin{pmatrix}x^5+250000x^4+5575\cdot10^7x^3+11215\cdot10^{12}x^2\\+2815140625\cdot10^{12}x-741200625\cdot10^{16}\end{pmatrix}$$

$\therefore$ $f_\beta(x)=0$ から、$x=250000$ が得られ、$\beta=250000$

これより、

$ps=-\sqrt{2500}/50=-1$

$qr=+\sqrt{2500}/50=+1$

また、p^2r と qs^2 を

$t^2-\left(\frac{-\sqrt{250000}}{250}\right)t+\frac{(-\sqrt{2500})^2(+\sqrt{2500})}{125000}=0$ の２解と考えると、

$t^2+2t+1=0$　より

$p^2r=-1$

$qs^2=-1$

また、pq^2 とr^2s　を

$t^2-\left(\frac{\sqrt{250000}}{250}\right)t+\frac{(-\sqrt{2500})(+\sqrt{2500})^2}{125000}=0$　の２解と考えると、

$t^2-2t-1=0$　より

$pq^2=1-\sqrt{2}$

$r^2s=1+\sqrt{2}$

よって、

$p^5=\frac{(p^2r)^2(pq^2)}{(qr)^2}=1-\sqrt{2}$

$q^5=\frac{(pq^2)^2(qs^2)}{(ps)^2}=-3+2\sqrt{2}$

$r^5=\frac{(r^2s)^2(p^2r)}{(ps)^2}=-3-2\sqrt{2}$

$s^5=\frac{(qs^2)^2(r^2s)}{(qr)^2}=1+\sqrt{2}$

$$p^3q=\frac{p^2r\cdot pq^2}{qr}=-1+\sqrt{2}\quad ,pr^3=\frac{p^2r\cdot r^2s}{ps}=\ 1+\sqrt{2}$$

$$q^3s=\frac{pq^2\cdot qs^2}{ps}=\ 1-\sqrt{2}\quad ,rs^3=\frac{qs^2\cdot r^2s}{qr}=-1-\sqrt{2}$$

これらを使うと (6),(7)式の

$$-5(p^3q+pr^3+q^3s+rs^3+pqrs-p^2s^2-q^2r^2)$$

$$=-5\begin{pmatrix}\dfrac{p^2r\cdot pq^2}{qr}+\dfrac{p^2r\cdot r^2s}{ps}+\dfrac{pq^2\cdot qs^2}{ps}+\dfrac{qs^2\cdot r^2s}{qr}\\+(ps)(qr)-(ps)^2-(qr)^2\end{pmatrix}=15=a_1$$

と

$$-(\,p^5+q^5+r^5+s^5)+5(\,ps-qr)(p^2r-pq^2+qs^2-r^2s)=44=a_0$$

の確認ができる。

これより

$$p=\ \sqrt[5]{1-\sqrt{2}}\ \fallingdotseq -0.838388$$

$$q=\ \sqrt[5]{-3+2\sqrt{2}}\fallingdotseq -0.702894$$

$$r=\sqrt[5]{-3-2\sqrt{2}}\ \fallingdotseq -1.42269$$

$$s=\ \sqrt[5]{1+\sqrt{2}}\ \fallingdotseq 1.19277$$

となって、

$x^5+15x+44=0$ の解は、ζ を 1 の原始 5 乗根

($\zeta=e^{\frac{2\pi i}{5}}=-\frac{1}{4}+\frac{\sqrt{5}}{4}+i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}}\ \fallingdotseq 0.309017+0.951057\,i$) として

$$x_1=p+q+r+s$$

$$\fallingdotseq -0.838388+(-0.702894)+(-1.42269)+1.19277=-1.77121$$

$$x_2=p\zeta^1+q\zeta^2+r\zeta^3+s\zeta^4$$

$$\fallingdotseq\ 1.82915-1.50866\,i$$

$$x_3=p\zeta^2+q\zeta^4+r\zeta^1+s\zeta^3$$

$$\fallingdotseq -0.94354-1.87845\,i$$

$x_4=\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

$x_5=\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$ が求まる。 （終）

(例 4)　$x^5+20x+32=0$　の解

（この方程式のガロア群は、D_{10} に同型）

$a_3=0$,$a_2=0$,$a_1=20$,$a_0=32$

また、

$$f_\alpha(x)=(x-2000)\begin{pmatrix} x^5-2000x^4+48\cdot 10^5x^3+64\cdot 10^7x^2 \\ +576\cdot 10^{10}x-512\cdot 10^{11} \end{pmatrix}$$

∴ $f_\alpha(x)=0$ から、$x=2000$ が得られ、$\alpha=2000$

$$f_\beta(x)==(x-200000)\begin{pmatrix} x^5+200000x^4+24\cdot 10^9x^3+224\cdot 10^{13}x^2 \\ +512\cdot 10^{18}x-8192\cdot 10^{21} \end{pmatrix}$$

∴ $f_\beta(x)=0$ から、$x=200000$ が得られ、$\beta=200000$

これより、

$$ps=+\sqrt{2000}/50\ =\frac{2\sqrt{5}}{5}$$

$$qr=-\sqrt{2000}/50\ =-\frac{2\sqrt{5}}{5}$$

また、p^2r と qs^2 を

$$t^2-\left(\frac{\sqrt{200000}}{250}\right)t+\frac{\left(+\sqrt{2000}\right)^2\left(-\sqrt{2000}\right)}{125000}=0$$

$\left(\ t^2-\frac{4\sqrt{5}}{5}\ t-\frac{8\sqrt{5}}{25}=0\ \right)$ の 2 解と考えると、

$$p^2r=\frac{2}{5}(\sqrt{5}-\sqrt{5+2\sqrt{5}}\,)$$

$$qs^2=\ \frac{2}{5}(\sqrt{5}+\sqrt{5+2\sqrt{5}}\,)$$

また、pq^2 と r^2s を

$$t^2-\left(\frac{-\sqrt{200000}}{250}\right)t+\frac{\left(+\sqrt{2000}\right)\left(-\sqrt{2000}\right)^2}{125000}=0$$

($t^2+\frac{4\sqrt{5}}{5}\ t+\frac{8\sqrt{5}}{25}=0$) の 2 解と考えると、

$$pq^2\ =-\frac{2}{5}(\sqrt{5}+\sqrt{5-2\sqrt{5}}\,)$$

$$r^2s=-\frac{2}{5}(\sqrt{5}-\sqrt{5-2\sqrt{5}}\,)$$

よって、

$$p^5=\frac{(p^2r)^2(pq^2)}{(qr)^2}=-\frac{2}{25}(\sqrt{5}+\sqrt{5-2\sqrt{5}})(\sqrt{5}-\sqrt{5+2\sqrt{5}})^2 \fallingdotseq -0.167877$$

$$q^5=\frac{(pq^2)^2(qs^2)}{(ps)^2}=\frac{2}{25}\left(\sqrt{5}+\sqrt{5-2\sqrt{5}}\right)^2(\sqrt{5}+\sqrt{5+2\sqrt{5}}) \fallingdotseq 3.73113$$

$$r^5=\frac{(r^2s)^2(p^2r)}{(ps)^2}=\frac{2}{25}\left(\sqrt{5}-\sqrt{5-2\sqrt{5}}\right)^2(\sqrt{5}-\sqrt{5+2\sqrt{5}}) \fallingdotseq -0.153421$$

$$s^5=\frac{(qs^2)^2(r^2s)}{(qr)^2}=-\frac{2}{25}\left(\sqrt{5}-\sqrt{5-2\sqrt{5}}\right)\left(\sqrt{5}+\sqrt{5+2\sqrt{5}}\right)^2 \fallingdotseq -3.40983$$

$$p^3q=\frac{p^2r\cdot pq^2}{qr}\quad ,pr^3=\frac{p^2r\cdot r^2s}{ps}\quad ,q^3s=\frac{pq^2\cdot qs^2}{ps}\quad ,rs^3=\frac{qs^2\cdot r^2s}{qr}$$

これらを使うと (6),(7)式の

$$-5(p^3q+pr^3+q^3s+rs^3+pqrs-p^2s^2-q^2r^2)$$

$$=-5\left(\begin{gathered}\frac{p^2r\cdot pq^2}{qr}+\frac{p^2r\cdot r^2s}{ps}+\frac{pq^2\cdot qs^2}{ps}+\frac{qs^2\cdot r^2s}{qr}\\+(ps)(qr)-(ps)^2-(qr)^2\end{gathered}\right)=20=a_1$$

と

$$-(p^5+q^5+r^5+s^5)+5(ps-qr)(p^2r-pq^2+qs^2-r^2s)=32=a_0$$

の確認ができる。

これより

$$p=\sqrt[5]{-\frac{2}{25}(\sqrt{5}+\sqrt{5-2\sqrt{5}})(\sqrt{5}-\sqrt{5+2\sqrt{5}})^2} \fallingdotseq -0.699839$$

$$q=\sqrt[5]{\frac{2}{25}(\sqrt{5}+\sqrt{5-2\sqrt{5}})^2(\sqrt{5}+\sqrt{5+2\sqrt{5}})} \fallingdotseq 1.30127$$

$$r=\sqrt[5]{\frac{2}{25}\left(\sqrt{5}-\sqrt{5-2\sqrt{5}}\right)^2(\sqrt{5}-\sqrt{5+2\sqrt{5}})} \fallingdotseq -0.687348$$

$$s=\sqrt[5]{-\frac{2}{25}(\sqrt{5}-\sqrt{5-2\sqrt{5}})(\sqrt{5}+\sqrt{5+2\sqrt{5}})^2} \fallingdotseq -1.27805$$

となって、

$x^5+20x+32=0$ の解は、ζ を 1 の原始 5 乗根

($\zeta=e^{\frac{2\pi i}{5}}=-\frac{1}{4}+\frac{\sqrt{5}}{4}+i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}} \fallingdotseq 0.309017+0.951057\,i$)として

$$x_1=p+q+r+s$$

$$\fallingdotseq -0.699839+1.30127+(-0.687348)+(-1.27805)=-1.363967$$

$$x_2=p\zeta^1+q\zeta^2+r\zeta^3+s\zeta^4$$

$$\fallingdotseq -1.10788+1.71879\,i$$

$$x_3 = p\zeta^2 + q\zeta^4 + r\zeta^1 + s\zeta^3$$
$$\fallingdotseq 1.78986 - 1.55143\,i$$
$$x_4 = \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$x_5 = \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

（終）

(例 5)　$x^5 - 110x^3 - 55x^2 + 2310x + 979 = 0$　の解

（この方程式のガロア群は、C_5 に同型）

$a_3 = -110$,$a_2 = -55$,$a_1 = 2310$,$a_0 = 979$

また、

$$f_\alpha(x) = x\begin{pmatrix} x^5 - 825000x^4 + 24578125 \cdot 10^4 x^3 - 311953125 \cdot 10^8 x^2 \\ +142978515625 \cdot 10^{10} x - 446807861328125 \cdot 10^{10} \end{pmatrix}$$

$\therefore\ f_\alpha(x) = 0$ から、$x = 0$ が得られ、$\alpha = 0$

$$f_\beta(x)$$
$$= (x - 236328125)\begin{pmatrix} x^5 - 274140625x^4 + 8432482910156250x^3 - 635165300369262695312 50x^2 \\ +96947815604507923126220703125x - 231449298124061897397041320801 78125 \end{pmatrix}$$

$\therefore\ f_\beta(x) = 0$ から、$x = 236328125$ が得られ、$\beta = 236328125$

これより、

$ps = 550/50 = 11$

$qr = 550/50 = 11$

また、

$p^2r + qs^2 = (25 \cdot 55 \pm \sqrt{236328125})/250 = (11 \pm 55\sqrt{5})/2$

$pq^2 + r^2s = (25 \cdot 55 \mp \sqrt{236328125})/250 = (11 \mp 55\sqrt{5})/2$

（複号同順）

また、

$(p^2r)(qs^2) = (ps)^2(qr) = 1331$

$(pq^2)(r^2s) = (ps)(qr)^2 = 1331$

これより、p^2r と qs^2 を

$t^2 - \left(\frac{11-55\sqrt{5}}{2}\right)t + 1331 = 0$　の２解とすると、

$$p^2r = \frac{11 - 55\sqrt{5} - 11\sqrt{-50 - 10\sqrt{5}}}{4}$$

$qs^2 = \frac{11-55\sqrt{5}+11\sqrt{-50-10\sqrt{5}}}{4}$

また、pq^2 とr^2s を

$t^2 - \left(\frac{11+55\sqrt{5}}{2}\right)t + 1331 = 0$ の２解とすると、

$$pq^2 = \frac{11+55\sqrt{5}+11\sqrt{-50+10\sqrt{5}}}{4}$$

$$r^2s = \frac{11+55\sqrt{5}-11\sqrt{-50+10\sqrt{5}}}{4}$$

これより、

$$p^5 = \frac{(p^2r)^2(pq^2)}{(qr)^2} = \frac{\left(11-55\sqrt{5}-11\sqrt{-50-10\sqrt{5}}\right)^2(11+55\sqrt{5}+11\sqrt{-50+10\sqrt{5}})}{7744}$$

$$q^5 = \frac{(pq^2)^2(qs^2)}{(ps)^2} = \frac{(11-55\sqrt{5}+11\sqrt{-50-10\sqrt{5}})\left(11+55\sqrt{5}+11\sqrt{-50+10\sqrt{5}}\right)^2}{7744}$$

$$r^5 = \frac{(r^2s)^2(p^2r)}{(ps)^2} = \frac{(11-55\sqrt{5}-11\sqrt{-50-10\sqrt{5}})\left(11+55\sqrt{5}-11\sqrt{-50+10\sqrt{5}}\right)^2}{7744}$$

$$s^5 = \frac{(qs^2)^2(r^2s)}{(qr)^2} = \frac{\left(11-55\sqrt{5}+11\sqrt{-50-10\sqrt{5}}\right)^2(11+55\sqrt{5}-11\sqrt{-50+10\sqrt{5}})}{7744}$$

$$p^3q = \frac{p^2r \cdot pq^2}{qr} \quad ,pr^3 = \frac{p^2r \cdot r^2s}{ps} \quad ,q^3s = \frac{pq^2 \cdot qs^2}{ps} \quad ,rs^3 = \frac{qs^2 \cdot r^2s}{qr}$$

これらを使うと (6),(7)式の

$$-5(p^3q + pr^3 + q^3s + rs^3 + pqrs - p^2s^2 - q^2r^2)$$

$$= -5\left(\begin{array}{c}\frac{p^2r \cdot pq^2}{qr} + \frac{p^2r \cdot r^2s}{ps} + \frac{pq^2 \cdot qs^2}{ps} + \frac{qs^2 \cdot r^2s}{qr} \\ +(ps)(qr) - (ps)^2 - (qr)^2\end{array}\right) = 2310 = a_1$$

と

$$-(p^5 + q^5 + r^5 + s^5) + 5(ps - qr)(p^2r - pq^2 + qs^2 - r^2s) = 979 = a_0$$

の確認ができる。

これより

$$p = \sqrt[5]{\frac{\left(11-55\sqrt{5}-11\sqrt{-50-10\sqrt{5}}\right)^2(11+55\sqrt{5}+11\sqrt{-50+10\sqrt{5}})}{7744}} \fallingdotseq -0.151715 + 3.31315\,i$$ (注 1)

$$q=\sqrt[5]{\frac{\left(11-55\sqrt{5}+11\sqrt{-50-10\sqrt{5}}\right)\left(11+55\sqrt{5}+11\sqrt{-50+10\sqrt{5}}\right)^2}{7744}}$$

$$\fallingdotseq 2.72879-1.88513\,i$$

$$r=\sqrt[5]{\frac{\left(11-55\sqrt{5}-11\sqrt{-50-10\sqrt{5}}\right)\left(11+55\sqrt{5}-11\sqrt{-50+10\sqrt{5}}\right)^2}{7744}}$$

$$\fallingdotseq 2.72879+1.88513\,i$$

$$s=\sqrt[5]{\frac{\left(11-55\sqrt{5}+11\sqrt{-50-10\sqrt{5}}\right)^2\left(11+55\sqrt{5}-11\sqrt{-50+10\sqrt{5}}\right)}{7744}}$$

$$\fallingdotseq -0.151715-3.31315\,i$$

(注 1)

《 $p^5 \fallingdotseq -91.0203+390.853\,i$ であり、p の値としては、

$(-3.19788+0.879531\,i)$,$(-1.82468-2.76957\,i)$,$(-0.151715+3.31315\,i)$

$(2.07016-2.59122\,i)$,$(3.10411+1.16811\,i)$ の 5 通りが考えられるが

$p=-0.151715+3.31315\,i$ を用いた。

q ,r ,s の値についても取捨選択している。 》

となって、

$x^5-110x^3-55x^2+2310x+979=0$ の解は、ζ を 1 の原始 5 乗根

($\zeta=e^{\frac{2\pi i}{5}}=-\frac{1}{4}+\frac{\sqrt{5}}{4}+i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}}\fallingdotseq 0.309017+0.951057\,i$)として

$$\begin{aligned}x_1&=p+q+r+s\\&\fallingdotseq(-0.151715+3.31315\,i)+(2.72879-1.88513\,i)+\\&\quad(2.72879+1.88513\,i)+(-0.151715-3.31315\,i)\\&=5.15415\end{aligned}$$

$$\begin{aligned}x_2&=p\zeta^1+q\zeta^2+r\zeta^3+s\zeta^4\\&\fallingdotseq -8.59493\end{aligned}$$

$$\begin{aligned}x_3&=p\zeta^2+q\zeta^4+r\zeta^1+s\zeta^3\\&\fallingdotseq -5.54861\end{aligned}$$

$$\begin{aligned}x_4&=p\zeta^3+q\zeta^1+r\zeta^4+s\zeta^2\\&\fallingdotseq 9.41254\end{aligned}$$

$$\begin{aligned}x_5&=p\zeta^4+q\zeta^3+r\zeta^2+s\zeta^1\\&\fallingdotseq -0.423148\end{aligned}$$

（終）

★　なお、$x^5-110x^3-55x^2+2310x+979=0$ の解は、

[$x^5-110x^3-55x^2+2310x+979 \equiv x^5 \quad (mod\ 11)$] であって、

1 の原始 11 乗根を ξ $(=e^{\frac{2\pi i}{11}} \fallingdotseq 0.841254+0.540641\,i)$ とすれば、

$x_1=5\xi^1+5\xi^{10}+1 \quad (\fallingdotseq 9.41254)$
$x_2=5\xi^2+5\xi^9+1 \quad (\fallingdotseq 5.15415)$
$x_3=5\xi^3+5\xi^8+1 \quad (\fallingdotseq -0.423148)$
$x_4=5\xi^4+5\xi^7+1 \quad (\fallingdotseq -5.54861)$
$x_5=5\xi^5+5\xi^6+1 \quad (\fallingdotseq -8.59493)$

$1:\ \xi^1 \to \xi^1$

$\sigma:\ \xi^1 \to \xi^2\ ,\xi^2 \to \xi^4\ ,\xi^3 \to \xi^6\ ,\xi^4 \to \xi^8\ ,\xi^5 \to \xi^{10}$
$\quad \xi^6 \to \xi^1\ ,\xi^7 \to \xi^2\ ,\xi^8 \to \xi^5\ ,\xi^9 \to \xi^7\ ,\xi^{10} \to \xi^9$

とすれば、

ガロア群は、$\{1,\sigma,\sigma^2,\sigma^3,\sigma^4\}$ で

$x_2=\sigma(x_1)\ ,x_4=\sigma^2(x_1)\ ,x_3=\sigma^3(x_1)\ ,x_5=\sigma^4(x_1)$

(例 5：$f(x)=x^5-110x^3-55x^2+2310x+979=0$) の別解

（この方程式のガロア群は、C_5 に同型）

ガロア群を$G=\{1,\sigma,\sigma^2,\sigma^3,\sigma^4\}$ とし、$f(x)=0$ の 1 つの解を α とすると、他の解は、$\sigma(\alpha)\ ,\sigma^2(\alpha)\ ,\sigma^3(\alpha)\ ,\sigma^4(\alpha)$ となる。

＜これより、しばらく $f(x)$ を $Q(\alpha)$ 上で因数分解することを考える＞（注 2）

$f(x)$ を $(x-\alpha)$ で割った式を $h(x)$ とすると、

$h(x)=x^4+\alpha x^3+(\alpha^2-110)x^2+(\alpha^3-110\alpha-55)x+$
$\quad \alpha^4-110\alpha^2-55\alpha+2310$

$h(x+\alpha)$ を計算し、x について整理すると

$h(x+\alpha,x)=x^4+5\alpha x^3+(10\alpha^2-110)x^2+(10\alpha^3-330\alpha-55)x+$
$\quad 5\alpha^4-330\alpha^2-110\alpha+2310$

$h(x+\alpha)$ を計算し、α について整理すると

$h(x+\alpha,\alpha)=5\alpha^4+10x\alpha^3+(10x^2-330)\alpha^2+$
$\quad (5x^3-330x-110)\alpha+x^4-110x^2-55x+2310$

$f(\alpha)$ と $h(x+\alpha,\alpha)$ の終結式 $r(x)$ を求め、因数分解すると、　（注 3）

$r(x)=(-34375+13750x-275x^3+x^5)(34375+13750x-275x^3+x^5)\times$
$(34375+6875x-1375x^2-275x^3+x^5)(-34375+6875x+1375x^2-275x^3+x^5)$

ここで、各因数を

$r_1(x) = -34375 + 13750x - 275x^3 + x^5$

$r_2(x) = \quad 34375 + 13750x - 275x^3 + x^5$

$r_3(x) = \quad 34375 + 6875x - 1375x^2 - 275x^3 + x^5$

$r_4(x) = -34375 + 6875x + 1375x^2 - 275x^3 + x^5$ 　　とおき、

はじめに、$h(x+\alpha, x)$ と $r_1(x)$, $r_2(x)$, $r_3(x)$, $r_4(x)$ の最大公約式 GCD を互除法で、それぞれ、（コンピューターを駆使して）順に、求めると、 (注 4)

（ただし、それぞれ、定数倍を無視してある）

$$x + \frac{-99 + 97\alpha + 3\alpha^2 - \alpha^3}{25}$$

$$x + \frac{-1276 - 71\alpha + 94\alpha^2 + 4\alpha^3 - \alpha^4}{125}$$

$$x + \frac{44 + 7\alpha - \alpha^2}{5}$$

$$x + \frac{671 + 36\alpha - 84\alpha^2 + \alpha^3 + \alpha^4}{125}$$

これらより

$$h(x+\alpha, x) = (x + \frac{-99 + 97\alpha + 3\alpha^2 - \alpha^3}{25})(x + \frac{-1276 - 71\alpha + 94\alpha^2 + 4\alpha^3 - \alpha^4}{125})$$

$$\times (\ x + \frac{44+7\alpha-\alpha^2}{5})(x + \frac{671+36\alpha-84\alpha^2+\alpha^3+\alpha^4}{125})$$

よって、

$f(x) = (x-\alpha)h(x)$

$$= (x-\alpha)\ (x - \alpha + \frac{-99+97\alpha+3\alpha^2-\alpha^3}{25})(x - \alpha + \frac{-1276-71\alpha+94\alpha^2+4\alpha^3-\alpha^4}{125})$$

$$\times (\ x - \alpha + \frac{44 + 7\alpha - \alpha^2}{5})(x - \alpha + \frac{671 + 36\alpha - 84\alpha^2 + \alpha^3 + \alpha^4}{125})$$

＜これで、$f(x)$ が $Q(\alpha)$ 上で因数分解できた。＞

次に、

$f(x) = 0$ のガロア群は、巡回群なので、$\{1, \sigma, \sigma^2, \sigma^3, \sigma^4\}$ とし、

$$s1 = \sigma(\alpha) = \alpha - \frac{44+7\alpha-\alpha^2}{5} = \frac{-44-2\alpha+\alpha^2}{5}$$ 　とおくと、

$$s2 = \sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \alpha - \frac{-1276-71\alpha+94\alpha^2+4\alpha^3-\alpha^4}{125} = \frac{1276+196\alpha-94\alpha^2-4\alpha^3+\alpha^4}{125}$$

$$s3 = \sigma^3(\alpha) = \alpha - \frac{-99 + 97\alpha + 3\alpha^2 - \alpha^3}{25} = \frac{99 - 72\alpha - 3\alpha^2 + \alpha^3}{25}$$

$$s4 = \sigma^4(\alpha) = \alpha - \frac{671 + 36\alpha - 84\alpha^2 + \alpha^3 + \alpha^4}{125} = \frac{-671 + 89\alpha + 84\alpha^2 - \alpha^3 - \alpha^4}{125}$$

となる。

そこで、ζ を１の原始５乗根とし、

$$\left(\zeta = e^{\frac{2\pi i}{5}} = -\frac{1}{4} + \frac{\sqrt{5}}{4} + i\sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}} \fallingdotseq 0.309017 + 0.951057\, i \right)$$

$u0 = \alpha + s1 \cdot 1 + s2 \cdot 1 + s3 \cdot 1 + s4 \cdot 1 = 0$

$u1 = \alpha + s1 \cdot \zeta^1 + s2 \cdot \zeta^2 + s3 \cdot \zeta^3 + s4 \cdot \zeta^4$

$u2 = \alpha + s1 \cdot \zeta^2 + s2 \cdot \zeta^4 + s3 \cdot \zeta^1 + s4 \cdot \zeta^3$

$u3 = \alpha + s1 \cdot \zeta^3 + s2 \cdot \zeta^1 + s3 \cdot \zeta^4 + s4 \cdot \zeta^2$

$u4 = \alpha + s1 \cdot \zeta^4 + s2 \cdot \zeta^3 + s3 \cdot \zeta^2 + s4 \cdot \zeta^1$　　とおくと、

コンピューターを使って、

$f(\alpha) = \alpha^5 - 110\alpha^3 - 55\alpha^2 + 2310\alpha + 979 = 0$,

$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$　　に注意すると、

$u1^5 = -893750 - 687500 \cdot \zeta + 515625 \cdot \zeta^2 - 343750 \cdot \zeta^3$

$u2^5 = -1409375 - 859375 \cdot \zeta - 1203125 \cdot \zeta^2 - 515625 \cdot \zeta^3$

$u3^5 = -550000 + 859375 \cdot \zeta + 343750 \cdot \zeta^2 - 343750 \cdot \zeta^3$

$u4^5 = -206250 + 687500 \cdot \zeta + 343750 \cdot \zeta^2 + 1203125 \cdot \zeta^3$

となることから、

$$\alpha = \frac{u0+u1+u2+u3+u4}{5}$$

$$= \frac{\sqrt[5]{-893750 - 687500 \cdot \zeta + 515625 \cdot \zeta^2 - 343750 \cdot \zeta^3}}{5}$$

$$+ \frac{\sqrt[5]{-1409375 - 859375 \cdot \zeta - 1203125 \cdot \zeta^2 - 515625 \cdot \zeta^3}}{5}$$

$$+ \frac{\sqrt[5]{-550000 + 859375 \cdot \zeta + 343750 \cdot \zeta^2 - 343750 \cdot \zeta^3}}{5}$$

$$+ \frac{\sqrt[5]{-206250 + 687500 \cdot \zeta + 343750 \cdot \zeta^2 + 1203125 \cdot \zeta^3}}{5}$$

$\fallingdotseq (2.72879 - 1.88513\, i) + (-0.151715 - 3.31315\, i)$

$+(-0.151715 + 3.31315\, i) + (2.72879 + 1.11513\, i)$

$= 5.15415$

★（ここで、注意しておくが、）

$u2^5 = -284439 - 1.22142 \cdot 10^6\, i$　であり、$u2$ の値としては、

$(-15.9894 - 4.39766\, i)$, $(-9.12341 + 13.8479\, i)$, $(-0.758573 - 16.5658\, i)$

$(10.3508+12.9561\,i)$,$(15.5206-5.84055\,i)$ の５通り考えられるが、

$-0.758573-16.5658\,i$ を選択している。

$u1$,$u3$,$u4$ の値についても取捨選択している。

残りの４つの解は、この α の値を次式に代入すればよい。

$$\sigma(\alpha)=\frac{-44-2\alpha+\alpha^2}{5}\fallingdotseq -5.54861$$

$$\sigma^2(\alpha)=\frac{1276+196\alpha-94\alpha^2-4\alpha^3+\alpha^4}{125}\fallingdotseq -0.423148$$

$$\sigma^3(\alpha)=\frac{99-72\alpha-3\alpha^2+\alpha^3}{25}\fallingdotseq -8.59493$$

$$\sigma^4(\alpha)=\frac{-671+89\alpha+84\alpha^2-\alpha^3-\alpha^4}{125}\fallingdotseq 9.41253$$ (終)

（注 2），（注 3），（注 4）をまとめて

（終結式とは）

s 次の $f(x)=0$ の解を $\alpha_1,\alpha_2,\dots\dots\dots,\alpha_s$ 、 t 次の $g(x)=0$ の解を $\beta_1,\beta_2,\dots\dots\dots,\beta_t$ とすれば、

$$f(x)=a_0x^s+a_1x^{s-1}+\cdots\cdots+a_s=a_0\prod_0^s(x-\alpha_i)$$

$$g(x)=b_0x^t+b_1x^{t-1}+\cdots\cdots+b_t=b_0\prod_0^t(x-\beta_j)$$

このとき、R= ${a_0}^s{b_0}^t\prod(\alpha_i-\beta_j)$,$(i=1,2,\dots.,s)$, $(j=1,2,\dots\dots,t)$ を

$f(x)$ と $g(x)$ の終結式($Resultant$)という。これは行列式でも求められる。

（定義から、$f(x)=0$ と $g(x)=0$ が共通解をもつ $\Leftrightarrow$ R=0 ）

(互除法で GCD を求める)

具体例で示す

$f(x)=3x^5+x^4-2x^3-6x^2-2x+4\ (=0)$ と

$g(x)=3x^4-5x^3+5x^2-5x+2\ (=0)$ の

最大公約式をユークリッドの互除法によって求めてみる。

$f(x)=(x+2)g(x)+r_1(x)$; $r_1(x)=3x^3-11x^2+6x$

$g(x)=(x+2)r_1(x)+r_2(x)$; $r_2(x)=21x^2-17x+2$

$r_1(x)=\left(\frac{x}{7}-\frac{20}{49}\right)r_2(x)+r_3(x)$; $r_3(x)=\frac{40}{49}-\frac{60x}{49}$

$r_2(x) = \left(\frac{49}{20} - \frac{343x}{20}\right) r_3(x) + 0$

$= \frac{-20}{49}\left(\frac{49}{20} - \frac{343x}{20}\right)(3x-2) + 0$

これより、最大公約式は、$(3x-2)$ である。

★実際に、

$f(x) = 3x^5 + x^4 - 2x^3 - 6x^2 - 2x + 4$

$= (x^3-2)(3x-2)(x+1)$

$g(x) = 3x^4 - 5x^3 + 5x^2 - 5x + 2$

$= (x^2+1)(3x-2)(x-1)$　より、GCD=$(3x-2)$

($Q(\alpha)$ 上での因数分解の要領)

５次式では繁雑になるので３次式で示す。

（５次式の場合も同様にすればできるが計算量はかなり多くなる。）

Q 上既約で、巡回群$(A_3 = C_3)$ をもつ、$f(x) = x^3 - 9x + 9$ の解の

１つを α とすると、

$f(x) = (x-\alpha)(x^2 + \alpha x + \alpha^2 - 9)$

ここで、$h(x) = x^2 + \alpha x + \alpha^2 - 9$ とおくと、

$h(x+\alpha) = x^2 + 3\alpha x + 3\alpha^2 - 9 \quad (= hh)$

$= 3\alpha^2 + 3x\alpha + x^2 - 9$

これと、$f(\alpha) = \alpha^3 - 9\alpha + 9 \quad (= 0)$ の終結式 R を考えると、

R=$x^6 - 54x^4 + 729x^2 - 729 = (x^3 - 27x + 27)(x^3 - 27x - 27)$

$r1 = x^3 - 27x + 27$　, $r2 = x^3 - 27x - 27$とし、はじめに

$r1$と hh との最大公約式 GCD$(r1, hh)$を互除法で考えと、

$r1 = (x - 3\alpha)hh + (6\alpha^2 - 18)x + 9\alpha^3 - 27\alpha + 27$

$s1 = (6\alpha^2 - 18)x + 9\alpha^3 - 27\alpha + 27$ とおくと、

$$hh = \left(\frac{(-9-9\alpha+3\alpha^3)+(-6+2\alpha^2)x}{12(-3+\alpha^2)^2}\right)\cdot s1 + 0$$

これより、

$$\mathrm{GCD}(r1, hh) = \frac{(-9-9\alpha+3\alpha^3)+(-6+2\alpha^2)x}{12(-3+\alpha^2)^2}$$

ここで、$\frac{1}{12(-3+\alpha^2)^2} = \frac{1}{12}\cdot\frac{1}{9-9\alpha+\alpha^3} = \frac{1}{12}\cdot\frac{9-\alpha^2}{27}$

$\therefore$ GCD$(r1, hh) = \frac{1}{12}\cdot\frac{9-\alpha^2}{27}\cdot\{(-9 - 9\alpha + 3\alpha^3) + (-6 + 2\alpha^2)x\}$

$$=\frac{1}{324}\cdot\{(-162+36\alpha^2)+(-54+18\alpha+6\alpha^2)x\}$$

ここで、$\frac{1}{-54+18\alpha+6\alpha^2}=\frac{15-11\alpha-\alpha^2+\alpha^3}{54}$

$$=\frac{1}{324}\cdot\left\{x+(-162+36\alpha^2)\cdot(\frac{15-11\alpha-\alpha^2+\alpha^3}{54})\right\}$$

これより、定数倍を無視すれば、

$\mathrm{GCD}(r1,hh)=x+(-\alpha^2+6)$

同様にして、

$\mathrm{GCD}(r2,hh)=x+(\alpha^2+3\alpha-6)$

これで、

$h(x+\alpha)=x^2+3\alpha x+3\alpha^2-9$

$\qquad=\{x+(-\alpha^2+6)\}\{x+(\alpha^2+3\alpha-6)\}$

$\therefore\quad h(x)=\{x+(-\alpha^2-\alpha+6)\}\{x+(\alpha^2+2\alpha-6)\}$

$\therefore\ f(x)=(x-\alpha)h(x)$

$\qquad=(x-\alpha)\{x+(-\alpha^2-\alpha+6)\}\{x+(\alpha^2+2\alpha-6)\}$

$\qquad=(x-\alpha)\{x-(\alpha^2+\alpha-6)\}\{x-(-\alpha^2-2\alpha+6)\}$ （終）

★参考までに

$\sigma(\alpha)=\alpha^2+\alpha-6$ とすれば、$\alpha^3-9\alpha+9=0$ に注意して

$\sigma^2(\alpha)=\sigma\big(\sigma(\alpha)\big)=-\alpha^2-2\alpha+6$

$\sigma^3(\alpha)=\sigma\Big(\sigma\big(\sigma(\alpha)\big)\Big)=\alpha=1(\alpha)$ となって、

$f(x)=0$ のガロア群は、巡回群 $\{1,\sigma,\sigma^2\}$ だと確認できる。

〘引用、参考文献〙

笠原　乾吉著「数学セミナー1988年7，8月号：モジュラー方程式とエルミートの解法」

退職後は素人数学者著「可解な代数方程式のガロア理論に基づいた解法」

元吉　文男著「数理解析研究所講究録722（1990年） p 17～20：巡回群をガロア群にもつ
5次方程式の判別とその方法」

山下純一著「ガロアへのレクイエム」

大迎　規宏著「平成15年度　学位論文　可解な5次方程式について」

小林　滋著「Mathematica Japonica Vol,37,No5,1992__Resolution of Solvable Quintic equation」

結城　浩著「数学ガール ガロア理論」

井汲景太氏による5次元世界の冒険「方程式のガロア群の求め方」

三森明夫著「ガロア論文の古典的証明」

阿部　英一著「代数学」

アルティン著「ガロア理論入門」寺田文行訳

石田　信著「代数学入門」

草場　公邦著「ガロアと方程式」

倉田　令二郎著「ガロアを読む」

スチュアート著「ガロア理論」新関章三訳

高木　貞二著「代数学講義」

一松　信著「代数系入門」

ファンデルヴェルデン著「現代代数学」銀林浩訳

藤崎　源二郎著「体と Galois 理論Ⅱ」

藤原　松三郎著「代数学第二巻」

細井　勉著「代数系入門」

増田　真朗著「代数系入門」

松坂　和夫著「代数系入門」

矢ケ部　厳著「数Ⅲ方式ガロア理論」