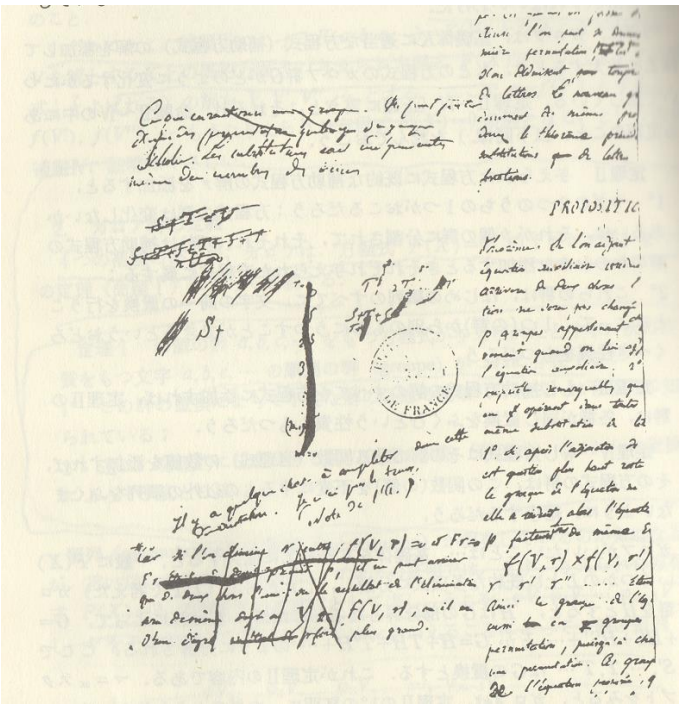
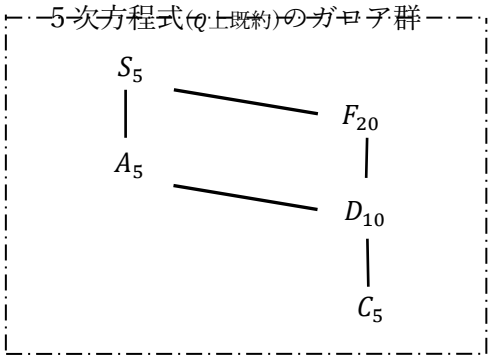
入門　５次方程式のガロア群



（仏 Evariste Galois 1811～1832）

４次方程式までは、四則演算と累乗根（ベキ根）をとることで一般式の解の公式を作れるが５次以上の方程式ではそれができないことを今でいう群や体の概念を用いて、彼 Galois（ガロア）が示した。

〖内容〗



はじめに。

◎　ガロア群とは（3，4 次方程式のガロア群でも述べたが）

有理数体 Q 上既約な（Q 内の係数をもつ）$f(x)=x^2-5=0$ は、
Q に$\sqrt{5}$ を添加した体 $Q(\sqrt{5})=\{a+b\sqrt{5}\,|a,b\in Q\}$ 上では、
$f(x)=(x-\sqrt{5})(x+\sqrt{5})=0$ のように
相異なる 1 次式の積に分解される。このとき、$L=Q(\sqrt{5})$ を
Q のガロア拡大といい、（下注 1）
L からそれ自身への自己同型写像、

$i:a+b\sqrt{5}\to a+b\sqrt{5}$　（単に $\sqrt{5}\to\sqrt{5}$ と表す）　と

$\sigma:a+b\sqrt{5}\to a-b\sqrt{5}$　（単に $\sqrt{5}\to-\sqrt{5}$ と表す）　の

集合 $\{i,\sigma\}$ は、群をなす。
これを方程式$f(x)=x^2-5=0$ または、多項式 $f(x)=x^2-5$ の
ガロア群(G)といい、$G=Q(L/Q)$ で表す。
この定義はガロア自身のものではないが、$f(x)=x^2-5=0$ の解を
$x_1=\sqrt{5}$,$x_2=-\sqrt{5}$ としたとき、

$i=\begin{pmatrix}x_1x_2\\x_1x_2\end{pmatrix}=\begin{pmatrix}12\\12\end{pmatrix}$　，$\sigma=\begin{pmatrix}x_1x_2\\x_2x_1\end{pmatrix}=\begin{pmatrix}12\\21\end{pmatrix}$

のように、解の置換群として捉えることができる。

<<注 1>>『 詳しくは、
体 K の拡大体 L がガロア拡大とは、分離拡大かつ正規拡大
であることをいう
有理数体 Q に$x^2-2=0$ の解 1 つ$\sqrt{2}$ を加えた体$Q(\sqrt{2})$ は
この上で $x^2-2=(x+\sqrt{2})(x-\sqrt{2})$となる（分離）ことや$\sqrt{2}$ と
共役な$(-\sqrt{2})$ を含んでいる（正規）ので Qのガロア拡大である。
有理数体 Q に$x^3-2=0$ の解 1 つ$\sqrt[3]{2}$ を加えた体 $Q(\sqrt[3]{2})$は
この上で$x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}\,x+\sqrt[3]{4})$ となるだけだし
$\sqrt[3]{2}$ と共役な$\sqrt[3]{2}\,\omega$ や$\sqrt[3]{2}\,\omega^2$（ω は 1 の虚数立方根)を含んでいない
から Qのガロア拡大でない。
ちなみに、$x^3-2=(x-\sqrt[3]{2})(x-\sqrt[3]{2}\,\omega)(x-\sqrt[3]{2}\,\omega^2)$ となる
ので $Q(\sqrt[3]{2}\,,\omega)$ は、 Qのガロア拡大である。　』

もう一例、ガロア群あげておく

Q 上既約な $f(x)=x^4+1=0$ は、

$Q(\sqrt{2}\,)$上で、 $f(x)=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)=0$ 、

$Q(\sqrt{-1}\,)=Q(\,i\,)$ 上で、 $f(x)=(x^2+i)(x^2-i)=0$ であるが

$Q(\sqrt{2}\,,i\,)=(Q(\sqrt{2}\,)(\,i\,)=\{s+t\,i\mid s\,,t\ \in Q(\sqrt{2}\,)\}$

$=\{a+b\sqrt{2}+c\,i+d\sqrt{2}\,i\ \big|\ a,b,c,d\ \in Q\}$ 上では

$f(x)=(x-x_1)(x-x_2)(x-x_3)(x-x_4)$

ただし、$x_1=(-1+i)/\sqrt{2}$ ，$x_2=(-1-i)/\sqrt{2}$

$x_3=(1+i)/\sqrt{2}$ ，$x_4=(1-i)/\sqrt{2}$

のように相異なる 1 次式の積に分解する。そこで

$Q(\sqrt{2}\,,i\,)$ からそれ自身への自己同型写像は、

$e:\ \sqrt{2}\ \to\sqrt{2}\ \ ,i\ \to\ i$

$\sigma:\ \sqrt{2}\ \to-\sqrt{2}\ \ ,i\ \to\ i$

$\tau:\ \sqrt{2}\ \to\sqrt{2}\ \ ,i\ \to-i$

$\tau\sigma:\ \sqrt{2}\ \to-\sqrt{2}\ \ ,i\ \to-i$ であり、

$x_1=1\ ,x_2=2\ ,x_3=3\ \ ,x_4=4$ とすれば、

$$e=\begin{pmatrix}1234\\1234\end{pmatrix}\ ,\sigma=\begin{pmatrix}1234\\4321\end{pmatrix}\ ,\tau=\begin{pmatrix}1234\\2143\end{pmatrix}\ ,\tau\sigma=\begin{pmatrix}1234\\3412\end{pmatrix}$$

この場合、ガロア群 $G=\{e\ ,\sigma\ ,\tau\ ,\tau\sigma\ \}\cong V$ ($Klein$ の 4 元群)

◎ 一般の 5 次方程式 $x^5+ax^4+bx^3+cx^2+dx+e=0$ は、

4 次式 $y=x^4+Ax^3+Bx^2+Cx+D$ をうまく選んで、この両辺から x を消去すると、 $y^5+Ky+L=0$ の形に変換できる。

これをチルンハウス ($Tschirnhaus$ 1651 – 1708) 変換と言う

((変換の手順))

① はじめに、3 次方程式の場合を考えてみる。

$$\begin{cases}x^3+ax^2+bx+c=0\\ \quad y=x^2+Ax+B\end{cases}$$

これらより、

$x^3=xx^2=x(y-Ax-B)=-ax^2-bx-c$

$\therefore\ xy-Ax^2-Bx=-ax^2-bx-c$

$\therefore\ (a-A)x^2=(-y+B-b)x-c$

$\therefore\ (a-A)(y-Ax-B)=(-y+B-b)x-c$

$\therefore\ (-A(a-A)+y-B+b)x=-(a-A)(y-B)-c$

$\therefore \quad x=\frac{-(a-A)(y-B)-c}{(-A(a-A)+y-B+b)}=\frac{(A-a)y-(A-a)B-c}{y+A(A-a)-B+b}$

これをもとの２番目の式に代入すると

$y=(\frac{(A-a)y-(A-a)B-c}{y+A(A-a)-B+b})^2+A(\frac{(A-a)y-(A-a)B-c}{y+A(A-a)-B+b})+B$

整頓すると

$y^3+m_1y^2+m_2y+m_3=0$　　（下注 2）

のような y に関する３次方程式が得られる。

ただし、ここで

$m_1=aA-3B-a^2+2b$

$m_2=bA^2+(-ab-2aB+3c)A+2a^2B-4bB+3B^2-2ac$

$m_3=cA^3+(-bB-ac)A^2+(abB+aB^2+bc-3Bc)A-b^2B$

$\quad -a^2B^2+2bB^2-B^3$

これより、$m_1=0$，$m_2=0$ となるように、A，B をとれば、

$y^3+K=0$ の形にできる。

このことは、m_1，m_2 の形から２次方程式を解くこと

なので可能である。

<<注 2>>

『　この式は、シルベスター（$Sylvester$ $1814-1897$）の消去法

による係数をとった行列式（終結式 $Resultant$）

$$\begin{vmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 1 & A & Z & 0 & 0 \\ 0 & 1 & A & Z & 0 \\ 0 & 0 & 1 & A & Z \end{vmatrix}=0$$　（ただし、$Z=B-y$）

からも求められる。　』

② ４次方程式の場合も３次と同じようにして

$y^4+L=0$ の形にできる。　（略）

③ ５次方程式の場合

$$\begin{cases} x^5+ax^4+bx^3+cx^2+dx+e=0 \\ y=x^4+Ax^3+Bx^2+Dx+E \end{cases}$$

$E-y=F$ としたとき、

$$\begin{vmatrix} 1 & a & b & c & d & e & 0 & 0 & 0 \\ 0 & 1 & a & b & c & d & e & 0 & 0 \\ 0 & 0 & 1 & a & b & c & d & e & 0 \\ 0 & 0 & 0 & 1 & a & b & c & d & e \\ 1 & A & B & D & F & 0 & 0 & 0 & 0 \\ 0 & 1 & A & B & D & F & 0 & 0 & 0 \\ 0 & 0 & 1 & A & B & D & F & 0 & 0 \\ 0 & 0 & 0 & 1 & A & B & D & F & 0 \\ 0 & 0 & 0 & 0 & 1 & A & B & D & F \end{vmatrix} = 0$$

これを解くと、y に関する 5 次方程式、

$y^5 + G_1 y^4 + G_2 y^3 + G_3 y^2 + G_4 y + G_5 = 0$ が得られる。

ただし、

$G_1 = (a^3 - 3ab + 3c)A + 4d + aD - 5E - a^4 +$
$4a^2 b - 2b^2 - a^2 B + 2bB - 4ac$

$G_2 = (b^3 - 3abc + 3c^2 + 3a^2 d - 3bd - 3ae)A^2 + (\cdots\cdots)A + \cdots\cdots$

$G_3 = (c^3 - 3bcd + 3ad^2 + 3b^2 e - 3ace - 3de)A^3 + (\cdots\cdots)A^2 +$
$(\cdots\cdots)A + \cdots\cdots\cdots$

$G_4 = (d^3 - 3cde + 3be^2)A^4 +$
$(-Bcd^2 - ad^3 + c^2 dD - 2bd^2 D + 2Bc^2 e + bBde +$
$3acde + d^2 e - bcDe + 5adDe - 3abe^2 - 4aBe^2 - 2ce^2 -$
$5De^2 - 2c^3 E + 6bcdE - 6ad^2 E - 6b^2 eE + 6aceE + 6deE)A^3 +$
$(\cdots\cdots)A^2 + (\cdots\cdots)A + \cdots\cdots$

（注　$G_k\ (k = 1,2,\ldots 5)$ は、A, B, D, E の k 次の同次式で
その係数は、a, b, c, d, e の整式である。）

この後、

$\begin{cases} G_1 = 0 \\ G_2 = 0 \\ G_3 = 0 \end{cases}$ を解けば、

$y^5 + Ky + L = 0$ の形が得られる。

（ここで注意することは、$G_4 = 0$ まで含めると
うまく 4 次以下の解法にもちこめなくなる。
従って $y^5 + M = 0$ の形までにはできない。）

このことは、4 次方程式まで、$X^2 = A$, $X^3 = K$, $X^4 = L$ と
できたので、暗に 5 次方程式がベキ根だけでは解けないことを
示しているかもしれない？

ここから

5次方程式のガロア群

5次方程式のガロア群は、チルンハウス変換によって理論上は
$x^5+ax+b=0$ の形になるのでこの形ものを考えることにする。

定理 1

Q 上既約な $f(x)=x^5+ax+b=0$ の解を $x_1\ ,x_2\ ,x_3\ ,x_4\ ,x_5$
とし、$D=\prod(\ x_i-x_j\ )^2$ （ただし、$1\le i<j\le 5$ ）とすると

(1) $D=\ 4^4a^5+5^5b^4$

(2) $D<0$ ならば、$f(x)=0$ は、3つの実数解（2つの虚数解）をもつ

((証明))

(1) $x_1\ ,x_2\ ,x_3\ ,x_4\ ,x_5$ は、$f(x)=0$ の解だから
$f(x)=(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)$ と書ける

$\therefore\quad f'(x)=(x-x_2)(x-x_3)(x-x_4)(x-x_5)$
$+(x-x_1)(x-x_3)(x-x_4)(x-x_5)$
$+(x-x_1)(x-x_2)(x-x_4)(x-x_5)$
$+(x-x_1)(x-x_2)(x-x_3)(x-x_5)$
$+(x-x_1)(x-x_2)(x-x_3)(x-x_4)$

$\therefore\quad f'(x_1)=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_1-x_5)$
$f'(x_2)=(x_2-x_1)(x_2-x_3)(x_2-x_4)(x_2-x_5)$
$f'(x_3)=(x_3-x_1)(x_3-x_2)(x_3-x_4)(x_3-x_5)$
$f'(x_4)=(x_4-x_1)(x_4-x_2)(x_4-x_3)(x_4-x_5)$
$f'(x_5)=(x_5-x_1)(x_5-x_2)(x_5-x_3)(x_5-x_4)$

一方、

$D=(x_1-x_2)^2(x_1-x_3)^2(x_1-x_4)^2(x_1-x_5)^{\ 2}$
$\times(x_2-x_3)^2(x_2-x_4)^2(x_2-x_5)^2$
$\times(x_3-x_4)^2(x_3-x_5)^2(x_4-x_5)^2$

$\therefore\quad D=\prod f'(x_k)\qquad(k=1,2,\cdots,5)$
$=\prod(5{x_k}^4+a)\qquad(k=1,2,\cdots,5)$
$=\prod\frac{(5{x_k}^5+ax_k)}{x_k}\qquad(k=1,2,\cdots,5)$
$=\prod\frac{(5(-ax_k-b)+ax_k)}{x_k}\qquad(k=1,2,\cdots,5)$

$=\prod \frac{(-4ax_k-5b)}{x_k}$　　$(k=1,2,\cdots,5)$

ここで

分子$=\prod(-4ax_k-5b)$　　$(k=1,2,\cdots,5)$

$=-(4ax_1+5b)(4ax_2+5b)(4ax_3+5b)(4ax_4+5b)(4ax_5+5b)$

$=-\{(4a)^5x_1x_2x_3x_4x_5$

$+(4a)^4(5b)(x_1x_2x_3x_4+\cdots\cdots+x_2x_3x_4x_5)$

$+(4a)^3(5b)^2(x_1x_2x_3+\cdots\cdots\cdots+x_3x_4x_5)$

$+(4a)^2(5b)^3(x_1x_2+\cdots\cdots\cdots\cdots+x_4x_5)$

$+(4a)(5b)^4(x_1+x_2+x_3+x_4+x_5)$

$+(5b)^5\ \}$

（ 解と係数との関係より）

$=-\{(4a)^5(-b)+(4a)^4(5b)a+0+0+0+(5b)^5\ \}$

$=-\{4^4a^5b+5^5b^5\ \}$

分母$=\prod x_k = x_1x_2x_3x_4x_5=-b$

$\therefore\quad D=\frac{-\{4^4a^5b+5^5b^5\}}{-b}=4^4a^5+5^5b^4$

(2)　$f(x)=0$ は、既約としたから、

x_1 ,x_2 ,x_3 ,x_4 ,x_5 は異なるとしてよい

また、

$D=(x_1-x_2)^2(x_1-x_3)^2(x_1-x_4)^2(x_1-x_5)^2$

$\times(x_2-x_3)^2(x_2-x_4)^2(x_2-x_5)^2$

$\times(x_3-x_4)^2(x_3-x_5)^2(x_4-x_5)^2$

であるから、

㋐　解が 5 つとも実数ならば、$D>0$

㋑　3 つの解が実数で 2 つの解が虚数（共役）ならば、

たとえば、x_1 ,x_2 ,x_3 を実数、x_4 ,x_5 を共役な複素数

としたとき、

$(x_1-x_4)(x_1-x_5)>0$

$(x_2-x_4)(x_2-x_5)>0$

$(x_3-x_4)(x_3-x_5)>0$

また、(x_4-x_5) は、純虚数で $(x_4-x_5)^2<0$

その他、(x_1-x_2)、(x_1-x_3) 、(x_2-x_3) は実数

以上より、$D<0$

㋒　1つの解が実数で4つの解が虚数（共役が2組）

ならば、たとえば、x_1 が実数、x_2 と x_3 、x_4 と x_5 が

それぞれ共役な複素数としたとき、

$(x_1-x_2)(x_1-x_3)>0$

$(x_1-x_4)(x_1-x_5)>0$

$(x_2-x_4)(x_3-x_5)>0$

$(x_2-x_5)(x_3-x_4)>0$

また、(x_2-x_3) は、純虚数で $(x_2-x_3)^2<0$

(x_4-x_5) は、純虚数で $(x_4-x_5)^2<0$

以上より、$D>0$

㋐、㋑、㋒ 以外に $f(x)=0$ の解の持ち方はなく

逆に、$D<0$ ならば、$f(x)=0$ は、3つの実数解と

2つの虚数解をもつ

定理 2

Q 上既約な素数 p 次の方程式 $f(x)=0$ がちょうど2つの虚数解をもつならば、そのガロア群 は、対称群 S_p に同型である

（証明）

$f(x)=0$ はQ 上で既約であるから、相異なる p 個の解

α_1 ,α_2 ,……,α_{p-2} ,β_1 ,β_2 をもつ。

（ただし、α_1 ,α_2 ,……,α_{p-2} は実数で β_1 ,β_2 は共役な複素数）

$f(x)$ のQ 上の最小分解体($f(x)$を一次式に分解できる最小の拡大体) を

K 、そのガロア群を$G=G(K/Q)$ とすれば、G は $f(x)=0$ の解全体の置換であるから、S_p の部分群 H と同型である。

$\alpha_1=\alpha$ とすると、$Q(\alpha)\subset K$ で、

$[Q(\alpha):Q]=\big(Q(\alpha)$の Q 上の拡大次数$\big)=p$ である。

∴　$|G|=(G$の位数$)=|K/Q|=|K/Q(\alpha)|\cdot|Q(\alpha)/Q|$ より

$|G|$ は、p で割り切れる。

$|G|$ は、$|S_p|=p!$ の約数だから、$|G|=p$

したがって、G は、位数 p の元 τ を含む。

また、G は、位数2 の元 $\sigma:\beta_1\rightarrow\beta_2$ をもつ。

そこで、H は τ に対応する位数 p の巡回置換$(1\ 2\ \ldots..\ p)$ と
σ に対応する互換 $(1\ 2)$ をもつと思ってよい。
この 2 つの置換によって、S_p が生成されるから（下注 3）
$H = S_p \qquad \therefore G \cong S_p$

<<注 3>>

『 n 次対称群 S_n の元は、たとえば、$\begin{pmatrix}1234\ldots..n\\2413\ldots..n\end{pmatrix} = (1\ 3)(2\ 3)(3\ 4)$

のように互換の積で表されるがその互換は、

$\sigma = (1\ 2)$ と $\tau = (1\ 2\ \ldots.n)$ によって、

$(2\ 3) = \tau\sigma\tau^{-1}\ ,(3\ 4) = \tau^2\sigma\tau^{-2}\ ,\ldots\ldots..,(n-1\ \ n) = \tau^{n-2}\sigma\tau^{-(n-2)}$

$(1\ 3) = (2\ 3)(1\ 2)(2\ 3)\ \ ,$

$(1\ 4) = (3\ 4)(1\ 3)(3\ 4)\ \ ,\ldots\ldots\ldots.,(1\ n) = (n-1\ n)(1\ n-1)(n-1\ n)$

ように作られる。これより

S_n は、$\sigma = (1\ 2)$ と $\tau = (1\ 2\ \ldots.n)$ で生成される。 』

定理 3　定理 1、2 より、

$f(x) = x^5 + ax + b = 0$ が Q 上既約であり、$D = 4^4a^5 + 5^5b^4 < 0$
ならば、$f(x) = 0$ のガロア群は、S_5（5 次対称群）と同型である。

（例 1）　$x^5 - 4x + 2 = 0$ のガロア群 G
これは整数の範囲内で既約であり、
Q 上で既約である。（$Gauss$ の補題）
$D = 4^4(-4)^5 + 5^5 2^4 = -212144 \qquad < 0$
これより、$G \cong S_5$

（例 2）　$x^5 - 2px + p = 0$　（P は素数）のガロア群 G
これは、第 2 項の係数が、p で割り切れ、
末項の係数が、p^2 で割り切れないから、
$Eisenstein$ の判定法より Q 上で既約である。
$D = 4^4(-2p)^5 + 5^5p^4 = (3125 - 8192p)p^4 < 0$
これより、$G \cong S_5$

定理 4

$f(x)=x^5+ax+b=0$（Q 上既約)のガロア群 G において、
$\sqrt{D}=\sqrt{4^4a^5+5^5b^4}\in Q$　ならば、$G\subseteq A_5$　（5 次交代群）

((証明))

仮定より、

$f(x)=0$ の解を　$x_1\ ,x_2\ ,x_3\ ,x_4\ ,x_5$ とすると

$$\sqrt{D}=(x_1-x_2)(\ (x_1-x_3)(\ x_1-x_4)(\ x_1-x_5)$$
$$\times(x_2-x_3)(x_2-x_4)(\ x_2-x_5)$$
$$\times(x_3-x_4)(\ x_3-x_5)(x_4-x_5)$$

$Q\subset Q(\sqrt{D}\ )\subset Q(\ x_1\ ,x_2\ ,x_3\ ,x_4\ ,x_5\ )$ より

$Q(\sqrt{D}\ )=L_0$　$,Q(\ x_1\ ,x_2\ ,x_3\ ,x_4\ ,x_5\ )=L$　とすれば

$G(\ L/L_0\ )=G'$ の任意の元 σ は、$\sqrt{D}$ を不変にするから

$\sigma(\ \sqrt{D}\ )=\sqrt{D}$

一方、$\sqrt{D}$ はその形から、A_5 (偶置換全体)の元によっても

変わらない。　ゆえに、$\sigma\in G'\cap A_5$

$\therefore\quad G'\subseteq G'\cap A_5$

特に、　$\sqrt{D}\in Q$ のとき、$L_0=Q$ で$G'=G$

$\therefore\quad G\subseteq G\cap A_5$

逆は当然だから、$G=G\cap A_5$　　$\therefore G\subseteq A_5$

$f(x)=0$ を Q 上既約な 5 次方程式とし、そのガロア群を Gとすれば、
G は可移群（下注 4）でその位数は 5 の倍数、しかも S_5 の部分群に
同型だから、$5!=120=5\times2^3\times3$ の約数である。これより、
G としては、一応、位数が、120 の S_5 , 60 の A_5 , 40, 30 , 20 (F_{20}), 15 ,
10 (D_{10}) ,5 (C_5) の 8 通り(4×2）ものが考えられるが、
A_5 が単純群（下注 5）であることなどを考え合わせると、G としては
次の S_5 , A_5 , F_{20} , D_{10} , C_5 の 5 通りのいずれかと同型である。

S_5　…　位数 120 の 5 次対称群（5 個の数の置換全体）
A_5　…　位数 60 の 5 次交代群（5 個の数の偶置換全体）
F_{20}　…　位数 20 の群

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

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

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

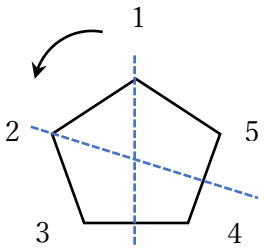
$\begin{pmatrix}12345\\14253\end{pmatrix}$ $\begin{pmatrix}12345\\25314\end{pmatrix}$ $\begin{pmatrix}12345\\31425\end{pmatrix}$ $\begin{pmatrix}12345\\42531\end{pmatrix}$ $\begin{pmatrix}12345\\53142\end{pmatrix}$ }

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。



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

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

C_5 … 位数 5 の巡回群

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

これを $<(12345)>$と表せば、

$<(12345)>=<(13524)>=<(14253)>=<(15432)>$である。

なお、D_{10} とF_{20} は、（例えば）次のようにも考えられる。

$D_{10}\cong C_5\cup\begin{pmatrix}12345\\15432\end{pmatrix}C_5$,$\begin{pmatrix}12345\\15432\end{pmatrix}$∈偶置換

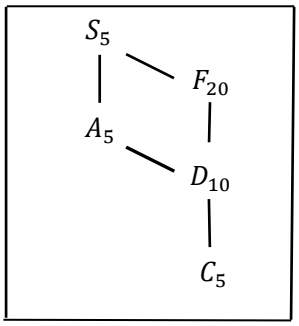
$F_{20}\cong D_{10}\cup\begin{pmatrix}12345\\13524\end{pmatrix}D_{10}$,$\begin{pmatrix}12345\\13524\end{pmatrix}$∈奇置換

また、$F_{20}\ni\begin{pmatrix}12345\\13524\end{pmatrix}=(2\ 4)(3\ 4)(4\ 5)\notin A_5$ より

$F_{20}\ \not\subset\ A_5$

以上から

Q 上既約な 5 次方程式のガロア群の包含関係は右図のようになる。



<<注 4 >>

『任意な $i, j \in X = \{1,2,\ldots.n\}$ に対して、$\sigma(i) = j$ となる $\sigma \in G$ が存在するとき、G を(X 上の)可移群という。

たとえば、 $X = \{1,2,3\}$ のとき

$\left\{\begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\231\end{pmatrix}, \begin{pmatrix}123\\312\end{pmatrix}\right\} = A_3$ や S_3 は、可移群であるが

$\left\{\begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\132\end{pmatrix}\right\} = H$ は置換群だが可移群でない。

$X = \{1,2,3\}$ 上の可移群は A_3 と S_3 であり、その位数は 3 の倍数。

なお、 Q 上既約な、$f(x) = 0$ のガロア群は可移群である。**(逆も成立)**

たとえば、Q 上既約な$x^3 - 3x + 1 = 0$ $\Leftrightarrow$ ガロア群 A_3 は可移的。

Q 上可約な$x^3 - 3x - 18 = (x-3)(x^2 + 3x + 6) = 0$

$\Leftrightarrow$ $x_1 = 3$と考えたとき,ガロア群 は$\left\{\begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\132\end{pmatrix}\right\}$で、可移的でない。 』

<<注 5 >>

『単純群とは、正規部分群として、それ自身と単位群$\{i\}$ しかもたないものをいう。ここで、H が G の正規部分群とは任意の $\sigma \in G$ に対し、$\sigma H = H\sigma$ が成り立つことである。

$A_3 = \left\{\begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\231\end{pmatrix}, \begin{pmatrix}123\\312\end{pmatrix}\right\}$ は S_3 の正規部分群である。

たとえば、$\sigma = \begin{pmatrix}123\\132\end{pmatrix} \in S_3$ に対して

$\sigma\begin{pmatrix}123\\123\end{pmatrix} = \begin{pmatrix}123\\132\end{pmatrix}\begin{pmatrix}123\\123\end{pmatrix} = \begin{pmatrix}123\\132\end{pmatrix}$, $\begin{pmatrix}123\\123\end{pmatrix}\sigma = \begin{pmatrix}123\\132\end{pmatrix}$

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

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

∴ この場合、 $\sigma A_3 = A_3\sigma$ 』

定理 5

『 有限体上の既約多項式(方程式)のガロア群は巡回群である 』

たとえば、

整数全体 Z の素数 p を法とした剰余類の集合（有限体）を

$F_p = \{0, 1, 2, \cdots\cdots, p-1\}$ で表すことにし、

$K = F_3 = \{0, 1, 2\}$ としたとき、

$f(x) = x^3 - x - 1$ は、K 上既約であり、(0, 1, 2 を代入してみるとよい)

α を $f(x) = 0$ の 1 解とすれば、$f(\alpha) = \alpha^3 - \alpha - 1 = 0$ で

残りの 2 解は、$\alpha + 1$, $\alpha + 2$ である。実際、

$f(\alpha + 1) = (\alpha + 1)^3 - (\alpha + 1) - 1 = \alpha^3 + 1 - \alpha - 1 + 1 = 0$

$f(\alpha + 2) = (\alpha + 2)^3 - (\alpha + 2) - 1 = \alpha^3 + 2 - \alpha - 2 + 1 = 0$

$K(\alpha) \ni \alpha, \alpha + 1, \alpha + 2$ はすべて異なるから、$f(x)$ は

分離多項式(重解がない)と言え、$K(\alpha)$ は K 上既約な $f(x)$ の

最小分解体 となり、K のガロア拡大である。

ガロア群 $G(K(\alpha)/K)$ は、

i ： $\alpha \to \alpha$ $\quad$ $(\alpha + 1 \to \alpha + 1$, $\alpha + 2 \to \alpha + 2)$

σ ： $\alpha \to \alpha + 1$ $\quad$ $(\alpha + 1 \to \alpha + 2$, $\alpha + 2 \to \alpha)$

σ^2 ： $\alpha \to \alpha + 2$ $\quad$ $(\alpha + 1 \to \alpha$, $\alpha + 2 \to \alpha + 1)$

であり、σ の生成する巡回群である。

(例 3) $f(x) = x^5 + 20x + 16 = 0$ のガロア群 G

これは、Q 上で既約であり

$D = 4^4(20)^5 + 5^5(16)^4 = 4^8 \cdot 5^6$

$\therefore \quad \sqrt{D} = 4^4 \cdot 5^3 \in Q$

$\therefore \quad G \subseteq A_5$

ここで、$f(x)$ を $mod\ 7$ で因数分解すると

$(x + 2)(x + 3)(x^3 + 2x^2 - 2x - 2)$ $\quad$ (下注 6)

これより、G は、3 項の巡回置換を含むことになる。(下注 7)

また、A_5 は 3 項の巡回置換から生成されるから $\quad$ (下注 8)

$G \cong A_5$

<<注 6 >> 実際に

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

$= x^5 + 7x^4 + 14x^3 - 22x - 12$

$\equiv x^5 + 20x + 16 \quad (mod\ 7)$

<<注 7 >>

n 次の整係数の既約多項式 $f(x)$ が、$mod\ p$ (p 素数)

で s 次、t 次、……の既約多項式に分解されるとき、

$f(x)$ のガロア群 G は、

（ s 項の巡回置換）×（ t 項の巡回置換）×……

の型の置換を含む。

<<注 8 >>

「 $n-2$ $(n \geq 3)$個の 3 項の巡回置換、$(1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 5), \ldots\ldots, (1\ 2\ n)$は A_n を生成する。 」

（証明）

S_n の元は、すべて互換 $(i\ j)$ の積として表され、

$(i\ j) = (1\ i)(1\ j)(1\ i)$ （ただし、$i \neq j$, $i \neq 1$, $j \neq 1$）

ここで、$j = 2$ なら $(1\ i)(1\ 2) = (1\ 2\ i)$

$i = 2$ なら $(1\ 2)(1\ j) = (1\ j\ 2) = (1\ 2\ j)^2$

$i\ , j \geq 3$ なら $(1\ i)(1\ j) = (1\ i)(1\ 2)(1\ 2)(1\ j)$

$= (1\ 2\ i)(1\ 2\ j)^2$

また、$(1\ 2\ k) = (1\ k)(1\ 2) \in A_n$ $(3 \leq k \leq n)$

これより A_n は、$(1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 5), \ldots\ldots, (1\ 2\ n)$ の形の巡回置換によって生成される。

（例 4）$f(x) = x^5 + 15x - 12 = 0$

これは、Q 上で既約であり

$D = 4^4(15)^5 + 5^5(-12)^4 = 4^4 \cdot 5^5 \cdot 3^4(3+1)$

$\therefore$ $\sqrt{D} = 4^2 \cdot 5^2 \cdot 3^2 \cdot 2\sqrt{5} = 7200\sqrt{5} \notin Q$

$\therefore$ $G \not\subset A_5$ $\therefore G \cong S_5$ か F_{20}

また、

$f(x) \equiv (x+1)(x^4 + 6x^3 + x^2 + 6x + 2)$ $(mod\ 7)$

$f(x) \equiv (x+5)(x^2 + 8x + 9)(x^2 + 9x + 10)$ $(mod\ 11)$

これらより、G は（4 項の巡回置換）と（ 互換の積）を含む。

$\therefore$ $G \cong F_{20}$

（例 5） $f(x) = x^5 + 20x - 32 = 0$

これは、Q 上で既約であり

$D = 4^4(20)^5 + 5^5(-32)^4 = 4^9 \cdot 5^5(1+4) = 2^{18} \cdot 5^6$

$\therefore$ $\sqrt{D} = 2^9 \cdot 5^3 = 64000 \in Q$

$\therefore$ $G \subseteq A_5$

また、$f(x) \equiv (x+10)(x^2+5x+3)(x^2+7x+7) \quad (mod\ 11)$

これより、G は互換の積を含む。

∴　$G \neq C_5$

∴　$\underline{G \text{ は、} D_{10} \text{ か} A_5}$　　$(F_{20} \not\subset A_5)$

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

$L = Q(\alpha_1, \alpha_2, \ldots\ldots, \alpha_5)$ を $f(x)$ の最小分解体とすると、

$\alpha_i + \alpha_j \quad (1 \leq i < j \leq 5)$ は、10 個の異なる L の元であり

$g(x) = \prod\left(x - (\alpha_i + \alpha_j)\right) \quad (1 \leq i < j \leq 5)$ を考えると

$f(x)=0$ のガロア群 $G = G(L/Q) \ni \sigma$ に対し

$$\sigma(g(x)) = \prod\left(x - (\sigma(\alpha_i) + \sigma(\alpha_j))\right)$$

$$= \prod\left(x - (\alpha_i + \alpha_j)\right) \quad \text{（全体として）}$$

$$= g(x)$$

∴　$g(x) \in Q[x]$　（Q 係数の多項式）

また、$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = 0$　（ 解と係数との間の関係）より

$$\alpha_1 = -(\alpha_2+\alpha_3) - (\alpha_4+\alpha_5)$$
$$\alpha_2 = -(\alpha_1+\alpha_3) - (\alpha_4+\alpha_5)$$
$$\cdots\cdots\cdots\cdots$$
$$\alpha_5 = -(\alpha_1+\alpha_2) - (\alpha_3+\alpha_4)$$

$\alpha_1, \alpha_2, \ldots\ldots, \alpha_5$ は、$\alpha_i + \alpha_j \quad (1 \leq i < j \leq 5)$ で書け

$Q(\alpha_1, \alpha_2, \ldots\ldots, \alpha_5) \subseteq Q(\alpha_i + \alpha_j)$

逆は、当然で $Q(\alpha_i + \alpha_j) \subseteq Q(\alpha_1, \alpha_2, \ldots\ldots, \alpha_5)$

∴　$L = Q(\alpha_1, \alpha_2, \ldots\ldots, \alpha_5) = Q(\alpha_i + \alpha_j)$

∴　L は、$g(x)$ の最小分解体にもなっている。

∴　$g(x)$ のガロア群も G である。

ここで、$f(x)=0$（または $g(x)=0$）のガロア群を A_5 と仮定すると

A_5 全体で、$g(x)=0$ の解、$\alpha_1 + \alpha_2 (= \beta_1), \alpha_1 + \alpha_3 (= \beta_2), \ldots\ldots$

$\alpha_4 + \alpha_5 (= \beta_{10})$ は、可移的（推移的）であるから、$g(x)$ は、

(Q 上)既約である。（注 4 を参照）

しかるに、$g(x)$ は、コンピューターを使って計算すると、

$$g(x) = x^{10} - 60x^6 + 352x^5 - 1600x^2 - 2560x - 1024$$
$$= (x^5 - 10x^3 + 20x^2 + 40x + 16) \times (x^5 + 10x^3 - 20x^2 - 64)$$

のとおり、(Q 上)可約だとわかる。（これは矛盾。）

よって、　$G \cong D_{10}$

（例 6）$f(x)=x^5+x^4-12x^3-21x^2+x+5=0$ のガロア群 G

コンピューターを使って計算すると、

$\sqrt{D}=\prod(\alpha_i-\alpha_j) \quad (1\le i<j\le 5)$

$=4805\in Q$

$\therefore \quad G\subseteq A_5$

$mod\ p$（素数）で分解を試みると、

$x^5+x^4+x^2+x+1 \quad (mod\ 2)$ 既約

$x^5+x^4+x+2 \quad (mod\ 3)$ 既約

$x(x+1)(x+3)^2(x+4) \quad (mod\ 5)$

$x^5+x^4+2x^3+x+5 \quad (mod\ 7)$ 既約

$x^5+x^4+10x^3+x^2+x+5 \quad (mod\ 11)$ 既約

$x^5+x^4+x^3+5x^2+x+5 \quad (mod\ 13)$ 既約

$x^5+x^4+5x^3+13x^2+x+5 \quad (mod\ 17)$ 既約

$x^5+x^4+7x^3+17x^2+x+5 \quad (mod\ 19)$ 既約

$x^5+x^4+11x^3+2x^2+x+5 \quad (mod\ 23)$ 既約

$x^5+x^4+17x^3+8x^2+x+5 \quad (mod\ 29)$ 既約

$(x+25)^5 \quad (mod\ 31)$

$(x+10)(x+18)(x+20)(x+31)(x+33) \quad (mod\ 37)$

$x^5+x^4+29x^3+20x^2+x+5 \quad (mod\ 41)$ 既約

……．

これより、（おそらく）G は 5 項の巡回置換以外の置換を含まないことになり、 $G\cong C_5$ （下注 9）

なお、(1 次) (1 次) (1 次) (1 次) (1 次)の mod 分解は、

(1 項の巡回置換)×……×(1 項の巡回置換)、つまり

恒等置換を意味する。

<<注 9 >>

『 実際、$G\cong C_5$ であることは次の通り。

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

解 $\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5$ は、実は

ζ を 1 の原始 31 乗根$(\zeta^{31}=1,\zeta\neq 1)$とすれば、

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

$\alpha_2=\zeta^3+\zeta^{15}+\zeta^{18}+\zeta^{13}+\zeta^{16}+\zeta^{28}$

$\alpha_3=\zeta^9+\zeta^{14}+\zeta^{23}+\zeta^8+\zeta^{17}+\zeta^{22}$

$\alpha_4=\zeta^{27}+\zeta^{11}+\zeta^7+\zeta^{24}+\zeta^{20}+\zeta^4$

$\alpha_5 = \zeta^{19} + \zeta^2 + \zeta^{21} + \zeta^{10} + \zeta^{29} + \zeta^{12}$

で表され、$Q(\zeta)$ からそれ自身への自己同型写像を

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

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

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

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

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

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

とすれば、

$\sigma(\alpha_1) = \alpha_2 \ , \sigma(\alpha_2) = \alpha_3 \ , \sigma(\alpha_3) = \alpha_4 \ , \sigma(\alpha_4) = \alpha_5 \ , \sigma(\alpha_5) = \alpha_1$

となる。

$f(x)$ の最小分解体 $Q(\alpha_1 \ , \alpha_2 \ , \ldots\ldots , \alpha_5)$は、

$$\alpha_2 = \frac{3{\alpha_1}^4 - {\alpha_1}^3 - 33{\alpha_1}^2 - 24\alpha_1 + 15}{5}$$

$$\alpha_3 = \frac{-2{\alpha_1}^4 - {\alpha_1}^3 + 22{\alpha_1}^2 + 31\alpha_1}{5}$$

$$\alpha_4 = \frac{{\alpha_1}^4 - 2{\alpha_1}^3 - 6{\alpha_1}^2 + 2\alpha_1 - 10}{5}$$

$$\alpha_5 = \frac{-2{\alpha_1}^4 + 4{\alpha_1}^3 + 17{\alpha_1}^2 - 14\alpha_1 - 10}{5}$$

と表されることから、$Q(\alpha_1 \ , \alpha_2 \ , \ldots\ldots , \alpha_5) = Q(\alpha_1)$ であって、

ガロア群$G = G(Q(\alpha_1)/Q)$ は、σ を$Q(\alpha_1)$ 上に制限した

$\sigma : \alpha_1 \to \alpha_2 \ , \alpha_2 \to \alpha_3 \ , \alpha_3 \to \alpha_4 \ , \alpha_4 \to \alpha_5 \quad \alpha_5 \to \alpha_1$

を用いて、$G = \{1 \ , \sigma \ , \sigma^2 \ , \sigma^3 \ , \sigma^4 \} \cong C_5$ 　』

〖まとめ〗

これまでのことから、

5次方程式のガロア群（その1）

Q 上既約な5次方程式$f(x)=x^5+ax+b=0$ のガロア群を G とし、$f(x)=0$ の判別式を$D=4^4a^5+5^5b^4$ としたとき、

(1) $D<0 \quad \Longrightarrow \quad G\cong S_5$

(2) $D>0$

① $\sqrt{D}\in Q \quad \rightarrow \quad G\subseteq A_5$

$\therefore \quad G\cong A_5$ か D_{10} か C_5

素数 p の mod 分解で、(1次)(2次)(2次)が得られ、

$g(x)=\prod\left(x-(\alpha_i+\alpha_j)\right) \quad (1\le i<j\le 5)$ において、

(α_1～α_5 は$f(x)=0$ の5つの解)

$g(x)$が既約 $\Longrightarrow \quad G\cong A_5$

$g(x)$が可約 $\Longrightarrow \quad G\cong D_{10}$

② $\sqrt{D}\notin Q \quad \rightarrow \quad G\not\subset A_5$

$\therefore \quad G\cong S_5$ か F_{20}

素数 p の mod 分解で、

$\begin{cases} (1次)(4次) \\ (1次)(2次)(2次) \end{cases} \Longrightarrow G\cong F_{20}$

(2次)(3次) $\Longrightarrow \quad G\cong S_5$

◎ Q 上既約な5次方程式を$f(x)=0$ とし、$f(x)$ の最小分解体をL とする。

このとき、$f(x)=0$ がガロア群 $G(L/Q)$ として F_{20}をもてば、

$f(x)=0$ の1つの解を α としたとき、$Q\subseteq Q(\alpha)\subseteq L$ において

$20=[L:Q]=[L:Q(\alpha)]\cdot[Q(\alpha):Q]=[L:Q(\alpha)]\cdot 5$

$\therefore \quad [L:Q(\alpha)]=4$

これより、$f(x)$ は、$Q(\alpha)$ 上で定数倍を除いて、

$f(x)=(x-\alpha)$(αを含む x についての4次式) と分解される。

たとえば、$f(x)=x^5+15x-12$

$=(x-\alpha)(x^4+\alpha x^3+\alpha^2x^2+\alpha^3x+\alpha^4+15)$

したがって、このような場合に$f(x)$ をある素数 p の mod 分解をすれば

(1次)(4次)の分解が得られる。

◎ 同様に考えると

$f(x)=0$ がガロア群 $G(L/Q)$ として D_{10}をもてば、$f(x)$ は、$Q(\alpha)$ 上で定数倍を除いて、$f(x)=(x-\alpha)$(αを含む x についての2次式)(αを含む x についての2次式)

と分解され、$f(x)$ をある素数 p の mod 分解をすれば、(1 次)(2 次)(2 次)の分解が得られる。また、$f(x)=0$ がガロア群 $G(L/Q)$ として C_5をもてば、$f(x)$ は、$Q(\alpha)$ 上で

定数倍を除いて、$f(x)=(x-\alpha)\left(\alpha\text{を含む }x\text{ についての 1 次式}\right)\left(\alpha\text{を含む }x\text{ についての 1 次式}\right)$

$\times\left(\alpha\text{を含む }x\text{ についての 1 次式}\right)\left(\alpha\text{を含む }x\text{ についての 1 次式}\right)$

と分解され、$f(x)$ をある素数 p の mod 分解をすれば、(1 次)(1 次)(1 次)(1 次)(1 次)の分解が得られる。

5 次方程式のガロア群（その 2）

素数 p の mod 分解をフルに使って分類すると以下のようになる。

ただし、.各場合において、(1 次)(1 次)(1 次)(1 次)(1 次)の分解も得られるはずだが、これは恒等置換が含まれることを意味するだけなので省く。

① 5 次……既約

(1 次)(4 次)

(2 次)(3 次)

(1 次)(1 次)(3 次)

(1 次)(2 次)(2 次)

(1 次)(1 次) (1 次) (2 次)

これらが得られるとき $\Longrightarrow$ $G\cong S_5$

*実質、(2 次)(3 次)が得られた時点で $G\cong S_5$

② 5 次……既約

(1 次)(1 次)(3 次)

(1 次)(2 次)(2 次)

これらが得られるとき $\Longrightarrow$ $G\cong A_5$

③ 5 次……既約

(1 次)(4 次)

(1 次)(2 次)(2 次)

これらが得られるとき $\Longrightarrow$ $G\cong F_{20}$

④ 5 次……既約

(1 次)(2 次)(2 次)

これらが得られるとき $\Longrightarrow$ $G\cong D_{10}$

⑤ 5 次……既約 $\Longrightarrow$ $G\cong C_5$

この方法によるガロア群の判定は、$mod\ (p)$ 分解の試行が有限回しか行えないから少し無理があるかもしれないが、二、三十回行えば、ほぼ確定できるであろう(?)。

((参考例))

① $f(x)=x^5-4x+2=0$ のガロア群 $G\cong S_5$

$f(x)\equiv x^5+2x+2$　既約　$(mod\ 3)$

$f(x)\equiv (x+1)(x^2+2x+3)(x^2+2x+4)$　$(mod\ 5)$

$f(x)\equiv (x^2+4x+6)(x^3+3x^2+3x+5)$　$(mod\ 7)$

$f(x)\equiv (x+8)(x+11)(x^3+7x^2+8)$　$(mod\ 13)$

$f(x)\equiv (x+7)(x^4+12x^3+11x^2+18x+3)$　$(mod\ 19)$

$f(x)\equiv (x+91)(x+204)(x+226)(x^2+250x+139)$　$(mod\ 257)$

$f(x)\equiv (x+551)(x+553)(x+587)(x+683)(x+702)$　$(mod\ 769)$

② $f(x)=x^5+20x+16=0$ のガロア群 $G\cong A_5$

$f(x)\equiv x^5+2x+1$　既約　$(mod\ 3)$

$f(x)\equiv (x+2)(x+3)(x^3+2x^2+5x+5)$　$(mod\ 7)$

$f(x)\equiv (x+17)(x^2+12x+14)(x^2+17x+2)$　$(mod\ 23)$

$f(x)\equiv (x+304)(x+397)(x+511)(x+648)(x+801)$　$(mod\ 887)$

③ $f(x)=x^5+15x-12=0$ のガロア群 $G\cong F_{20}$

$f(x)\equiv (x+1)(x^4+6x^3+x^2+6x+2)$　$(mod\ 7)$

$f(x)\equiv (x+5)(x^2+8x+9)(x^2+9x+10)$　$(mod\ 11)$

$f(x)\equiv x^5+15x+7$　既約　$(mod\ 19)$

$f(x)\equiv (x+87)(x+88)(x+203)(x+220)(x+245)$　$(mod\ 281)$

④ $f(x)=x^5+20x-32=0$ のガロア群 $G\cong D_{10}$

$f(x)\equiv x^5+2x+1$　既約　$(mod\ 3)$

$f(x)\equiv (x+10)(x^2+5x+3)(x^2+7x+7)$　$(mod\ 11)$

$f(x)\equiv (x+65)(x+131)(x+135)(x+229)(x+247)$　$(mod\ 269)$

⑤ $f(x)=x^5+x^4-12x^3-21x^2+x+5=0$ のガロア群 $G\cong C_5$

$f(x)\equiv x^5+x^4+x^2+x+1$　$(mod\ 2)$

$f(x)\equiv x^5+x^4+x+2$　$(mod\ 3)$

$f(x)\equiv (x+10)(x+18)(x+20)(x+31)(x+33)$　$(mod\ 37)$

【参考までに】

３次方程式と４次方程式のガロア群の判定を素数 p の mod 分解を
フルに使って分類すると以下のようになる
（ただし、(１次)(１次)…(１次)の分解は省く）

３次方程式のガロア群 G

素数 p の mod 分解で

① ３次… 既約 と
(１次)(２次) が得られる ➡ $G \cong S_3$

② ３次… 既約 が得られる ➡ $G \cong A_3$

４次方程式のガロア群 G

素数 p の mod 分解で

① ４次… 既約 と
(１次)(１次)(２次) と
(１次)(3次) と
(2次)(２次) が得られる ➡ $G \cong S_4$

② (１次)(3次) と
(2次)(２次) が得られる ➡ $G \cong A_4$

③ ４次… 既約 と
(１次)(１次)(２次) と
(2次)(２次) が得られる ➡ $G \cong D_4$

（ここで、D_4は位数８の群で、正４角形をそれ自身に移す回転変換や鏡映変換）

④ (2次)(２次) だけが得られる ➡ $G \cong V$

（ここで、Vは位数４の群で、長方形をそれ自身に移す対称変換）

⑤ ４次… 既約 と
(2次)(２次) が得られる ➡ $G \cong C_4$

（ここで、C_4は位数４の巡回群）

〖引用、参考文献〗

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　巌著「数III方式ガロア理論」
山下純一著「ガロアへのレクイエム」
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」
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」