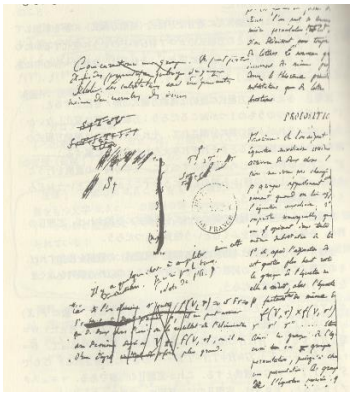
入門 3,4 次方程式のガロア群



ガロア（仏 Evariste Galois 1811～1832）

1811 年 10 月 25 日、パリ郊外のブール・ラ・レーヌに生まれるが
1832 年 5 月 31 日、銃による決闘に敗れ、20 歳 7 か月という若さで死亡
1830 年、後世に影響を与えることになる論文を発表

・根号によって方程式が解けるための条件について（第 1 論文）
[*Sur les conditions de resolubilite des equations par radicaux*]
・根号によって解ける原始方程式（第 2 論文）
[*Des equations primitives qui sont solubles par radicaux*]

〖内容〗

○ はじめに　　（p3～p4 ）

○ 3 次方程式のガロア群　　（p5～p18 ）

《 Q 上既約な 3 次方程式 》

（例 1） $x^3-21x+14=0$ のガロア群G $(\cong S_3)$

（例 2） $x^3-21x+7=0$ のガロア群G $(\cong A_3)$

《 Q 上可約な 3 次方程式 》

（例 3） $x^3-21x+36=0$ のガロア群G $(\cong S_2)$

（例 4） $x^3-2x^2-x+2=0$ のガロア群G $(\cong \{e\})$

○ 4 次方程式のガロア群　　（p19～p45 ）

《 Q 上既約な 4 次方程式 》

（例 1） $x^4+2x^2+12x+10=0$ のガロア群G $(\cong V)$

（例 2） $x^4+2x^2+8x+11=0$ のガロア群G $(\cong D_4)$

（例 3） $x^4+2x^2+8x+9=0$ のガロア群G $(\cong A_4)$

（例 4） $x^4+2x^2+8x+16=0$ のガロア群G $(\cong S_4)$

（例 5） $x^4+x^3+x^2+x+1=0$ のガロア群G $(\cong C_4)$

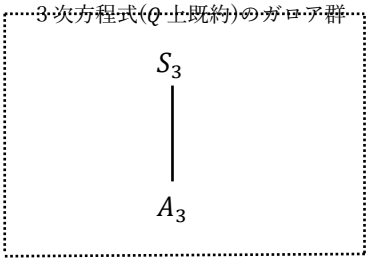
《 Q 上可約な 4 次方程式 》

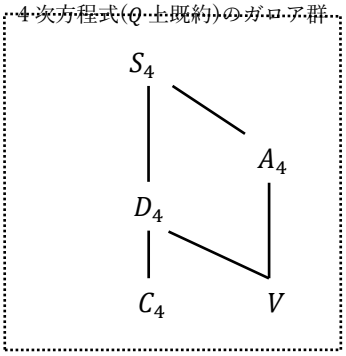
（例 6） $x^4-5x^2+6=0$ のガロア群G $(\cong V)$

（例 7） $x^4-x^3+x^2-1=0$のガロア群G $(\cong S_3)$

（例 8） $x^4+x^2+1=0$ のガロア群G $(\cong S_2)$

○ 引用、参考文献　　（p46）





はじめに。

$x^2-6x+7=0$ は有理数体 Q 上(Qの元を係数にもつ)では既約であるが
Q に$\sqrt{2}$を添加した拡大体 $L=Q(\sqrt{2})$=$\{a+b\sqrt{2} \mid a,b \in Q\}$ 上では、
$(x-(3+\sqrt{2}))(x-(3-\sqrt{2}))$ と 1 次式の積に分解する。
このとき、$Q(\sqrt{2})$ から$Q(\sqrt{2})$ への自己同型写像 σ (注 1)を考えると、
$a,b \in Q$ に対し、$\sigma(a+b\sqrt{2})=\sigma(a)+\sigma(b\sqrt{2})=a+b\sigma(\sqrt{2})$
ここで、$\sigma(\sqrt{2})^2=\sigma(\sqrt{2})\sigma(\sqrt{2})=\sigma(\sqrt{2}\sqrt{2})=\sigma(2)=2$
$\therefore \quad \sigma(\sqrt{2})=\pm\sqrt{2} \quad \therefore\sigma(a+b\sqrt{2})=a+b\sqrt{2}$ または $a-b\sqrt{2}$
これより、σ としては、
$\sigma_0=i$： $a+b\sqrt{2} \rightarrow a+b\sqrt{2}$ $(a,b \in Q)$ （単に$\sqrt{2}\rightarrow\sqrt{2}$ と略記）
$\sigma_1=\sigma$： $a+b\sqrt{2} \rightarrow a-b\sqrt{2}$ $(a,b \in Q)$ （単に$\sqrt{2}\rightarrow-\sqrt{2}$ と略記）
この $\{i\ ,\ \sigma\}$ を $x^2-6x+7=0$ のガロア群 $G=G(L/Q)$という。(注 2)
これは、$\alpha=a+b\sqrt{2}$, $\beta=a-b\sqrt{2}$ とすると、

$i=\begin{pmatrix}\alpha & \beta\\ \alpha & \beta\end{pmatrix}=\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$, $\sigma=\begin{pmatrix}\alpha & \beta\\ \beta & \alpha\end{pmatrix}=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$ であり、

$\{i\ ,\ \sigma\} \cong S_2$ (2 次対称群)

これをガロア流(注 3)によって求めてみる。
$x^2-6x+7=0$ の解を $\alpha,\ \beta$ とし、$V_1=\alpha+2\beta$ $(=\mathrm{V})$とおくと、
$\alpha+\beta=6$ より $\alpha=-V_1+12$ $,\beta=V_1-6$
また $V_2=\beta+2\alpha$ とおくと、$\alpha=V_2-6$ $,\beta=-V_2+12$
ここで、$\varphi_1(x)=-x+12$ $,\varphi_2(x)=x-6$ としたとき、
$\varphi_1(V_1)=-V_1+12=\alpha$ $,\varphi_2(V_1)=V_1-6=\beta$
$\varphi_1(V_2)=-V_2+12=\beta$ $,\varphi_2(V_2)=V_2-6=\alpha$
よって

$\begin{pmatrix}\varphi_1(V) & \varphi_2(V)\\ \varphi_1(V_1) & \varphi_2(V_1)\end{pmatrix}=\begin{pmatrix}\alpha & \beta\\ \alpha & \beta\end{pmatrix}=\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$

$\begin{pmatrix}\varphi_1(V) & \varphi_2(V)\\ \varphi_1(V_2) & \varphi_2(V_2)\end{pmatrix}=\begin{pmatrix}\alpha & \beta\\ \beta & \alpha\end{pmatrix}=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$

これらは、S_2 に同型。

(注 1) Kを体、$\alpha\ ,\beta \in K$ とし、Kからそれ自身への写像 σ が
$\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$, $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$ を満たすとき
σ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。単位元は恒等写像 i で
逆元は逆写像、写像の合成は結合律を満たす。
このとき、$\sigma(0)=0$, $\sigma(1)=1$, $\sigma(\alpha-\beta)=\sigma(\alpha)-\sigma(\beta)$
$\sigma(\alpha/\beta)=\sigma(\alpha)/\sigma(\beta)$ が成り立つ。
また、$a\in Q$ とすると$\sigma(a)=a$ （注 9）
（Qの元「有理数」は、どのような自己同型写像 σ でも不変）

（注 2）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をLのK上のガロア群といい、$G(L/K)$で表す。
体K上の分離多項式$f(x)$の最小分解体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。

ここで、

分解体：

体K上の既約多項式$f(x)$がKの拡大体L上では 1 次因数の積に分解するときLを$f(x)$の分解体といい、そのうち最小のものを最小分解体という。
たとえば、Q上既約な x^2-6x+7の最小分解体は$Q(\sqrt{2})$である。

分離多項式：

多項式$f(x)$がある分解体の中で相異なる 1 次因数の積に分解されるとき、それを分離多項式という。Q上既約な多項式は、すべて分離多項式である。

（注 3）ガロアによる作り方（3 次の場合）
$f(x)=0$ の解をα,β,γ としたとき、これを使って、Vを構成する。
（たとえば、$V=\alpha+2\beta+3\gamma$ ）。S_3 の 3!=6 通りの置換でVの値を入れ替えたものを$V_1(=V),V_2,\cdots\cdots,V_6$とし、$V_1,V_2,\cdots\cdots,V_6$ を解にもつ方程式$F(x)=(x-V_1)\cdots\cdots(x-V_6)$ を作る。これが既約である場合と可約である場合に分かれるが既約である場合、
これより、$\alpha=\varphi_1(V)$, $\beta=\varphi_2(V)$, $\gamma=\varphi_3(V)$ と表せて、
V を$V_1,V_2,\cdots\cdots,V_6$ に変えることで、6 個の順列が得られる。
この順列の生み出す置換群がガロア群である。

3 次方程式のガロア群

3 次方程式 $ax^3+bx^2+cx+d=0$ は、$x=y-\frac{b}{3a}$ とおくことで

$y^3+sy+t=0$ の形に書けるので、有理数体 Q 上(Qの元を係数にもつ)で

既約な$x^3+px+q=0$ 形のものを考えれば十分である。

Q上既約な$f(x)=x^3+px+q=0$ において$f(x)$ の最小分解体を

$L=Q(\alpha,\beta,\gamma)$ とし、$f(x)=(x-\alpha)(x-\beta)(x-\gamma)$ とするとき

$D=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$ とすれば、

$\alpha+\beta+\gamma=0$, $\alpha\beta+\beta\gamma+\gamma\alpha=p$, $\alpha\beta\gamma=-q$ より

$D=-4p^3-27q^2$ となって、$D\in Q$

また、$\sqrt{D}=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$

$=(\alpha^2-(\beta+\gamma)\alpha+\beta\gamma)(\beta-\gamma)$

$=(p+3\alpha^2)(\beta-\gamma)$

$\therefore \quad \beta-\gamma=\sqrt{D}(p+3\alpha^2)^{-1}$

一方、$\beta+\gamma=-\alpha$

$\therefore \quad \beta\,,\ \gamma\in Q(\alpha,\sqrt{D})$

$\therefore \quad Q(\alpha,\beta,\gamma)\subseteq Q(\alpha,\sqrt{D})$

逆は、$\sqrt{D}=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$ より

$\therefore \quad Q(\alpha,\sqrt{D})\subseteq Q(\alpha,\beta,\gamma)$

$\therefore \quad Q(\alpha,\beta,\gamma)=Q(\alpha,\sqrt{D})$

ここで、$f(x)=0$ のガロア群 $G(L/Q)$は、S_3の部分群に同型

であって、その位数は 6 の約数である。

これにより、

① $\sqrt{D}\in Q$ ならば、$L=Q(\alpha,\sqrt{D})=Q(\alpha)$ となり

$(L/Q)=(Q(\alpha)/Q)=3$ （注 4）

$\therefore\ |G(L/Q)|=(L/Q)=3$ （注 5）

$\therefore\ G(L/Q)\cong A_3$ （位数が 3 なのは 3 次交代群）

（注 4） $(\boldsymbol{L/Q})$は、LをQ 上のベクトル空間とみたときの L のQ 上の

拡大次数を表す。$[\boldsymbol{L:Q}]$ と表すことも多いがここでは、

以下 $(\boldsymbol{L/Q})$ のように表すことにする。

たとえば、 $\sqrt{2}$ はQ上既約な最小多項式

$x^2-2=0$ の解なので、$(Q(\sqrt{2})/Q)=2$

（注 5）L をK のガロア拡大(*)とするとき、　$|G(L/K)|=(L/K)$ (**)

すなわち、**ガロア群の位数＝拡大次数**　が成り立つ。

(*) 体 K上の既約多項式$f(x)$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。 たとえば、$\omega=(-1+\sqrt{-3})/2$

としたとき、$x^3-2=\left(x-\sqrt[3]{2}\right)\left(x^2+\sqrt[3]{2}x+\sqrt[3]{4}\right)$

$=(x-\sqrt[3]{2})(x-\sqrt[3]{2}\omega)(x-\sqrt[3]{2}\omega^2)$　なので $Q(\sqrt[3]{2})$は

Qのガロア拡大ではないが、$Q(\sqrt[3]{2},\omega)$は、Q のガロア拡大。

(**)たとえば、　$L=Q\left(\sqrt{2},\sqrt{3}\right)$, $K=Q$ としたとき、

$L=Q\left(\sqrt{2},\sqrt{3}\right)=\left(Q\left(\sqrt{2}\right)\right)\left(\sqrt{3}\right)=\{p+q\sqrt{3}\mid p,q\in Q\left(\sqrt{2}\right)\}$

$=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\mid a,b,c,d\in Q\}$　からそれ自身へ

の自己同型写像 σ を考えると

$\sigma\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\right)$ で $\sigma\left(\sqrt{2}\right)=\sqrt{2}$ または$-\sqrt{2}$ 、

$\sigma\left(\sqrt{3}\right)=\sqrt{3}$ または$-\sqrt{3}$ より、

σ_0： $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\ \rightarrow\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}$

（今後 $\sqrt{2}\rightarrow\sqrt{2}$,$\sqrt{3}\rightarrow\sqrt{3}$ と略記）

σ_1： $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\ \rightarrow\ a-b\sqrt{2}+c\sqrt{3}-d\sqrt{2}\sqrt{3}$

（今後 $\sqrt{2}\rightarrow-\sqrt{2}$,$\sqrt{3}\rightarrow\sqrt{3}$ と略記）

σ_2： $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\ \rightarrow\ a+b\sqrt{2}-c\sqrt{3}-d\sqrt{2}\sqrt{3}$

（今後 $\sqrt{2}\rightarrow\sqrt{2}$,$\sqrt{3}\rightarrow-\sqrt{3}$ と略記）

σ_3： $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\ \rightarrow\ a-b\sqrt{2}-c\sqrt{3}+d\sqrt{2}\sqrt{3}$

（今後 $\sqrt{2}\rightarrow-\sqrt{2}$,$\sqrt{3}\rightarrow-\sqrt{3}$ と略記）

∴　$G(L/K)=G(L/Q)=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3\}$　　∴ $|G(L/K)|=4$

一方、$L=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in Q\}$ を

Q上のベクトル空間とみなしたときの基底は、$1,\sqrt{2},\sqrt{3},\sqrt{6}$

の 4 個であり、拡大次数は 4 である。(***)

∴　$(L/K)=(L/Q)=4$　　したがって、　$|G(L/K)|=(L/K)$

(***)　次のことからもわかる。

$\alpha=\sqrt{2}+\sqrt{3}$ とすると $\alpha\in Q(\sqrt{2},\sqrt{3})$ $\therefore Q(\alpha)\subseteq Q(\sqrt{2},\sqrt{3})$

また、$(\alpha-\sqrt{2})^2=3$　∴ $\alpha^2-2\sqrt{2}\alpha-1=0$

∴ $\sqrt{2}=(\alpha^2-1)/2\alpha$　　∴ $\sqrt{2}\in Q(\alpha)$

∴ $\sqrt{3}=\alpha-\sqrt{2}\ \in Q(\alpha)$　∴　$Q(\sqrt{2},\sqrt{3})\subseteq Q(\alpha)$

したがって、$L=Q\left(\sqrt{2},\sqrt{3}\right)=Q\left(\sqrt{2}+\sqrt{3}\right)$

ここで、$\alpha=\sqrt{2}+\sqrt{3}$ は、Q 上既約な最小多項式

$x^4-10x^2+1=0$ の解であり、　$(Q(\sqrt{2}+\sqrt{3})/Q)=4$

② $\sqrt{D} \notin Q$ ならば、$\sqrt{D}$ は、Q上既約な$x^2 - D = 0$ の
解と考えられ、$(Q(\sqrt{D})/Q)=2$
∴ $(L/Q)=(Q(\alpha, \sqrt{D})/Q)$
$= (Q(\alpha, \sqrt{D})/Q(\alpha)) \times (Q(\alpha)/Q)$
$=2\times 3 = 6$
∴ $|G(L/Q)|=(L/Q)=6$
∴ $G(L/Q) \cong S_3$ （位数が 6 なのは 3 次対称群）

＜3 次方程式のガロア群_まとめ＞

Q上既約な$f(x) = x^3 + px + q = 0$ においては、
$D=-4p^3 - 27q^2$ であって、L を$f(x)$の最小分解体とするとき
① $\sqrt{D} \in Q \implies$ ガロア群 $G(L/Q) \cong A_3$
② $\sqrt{D} \notin Q \implies$ ガロア群 $G(L/Q) \cong S_3$

ここで、

$$A_3 = \left\{\begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\231\end{pmatrix}, \begin{pmatrix}123\\312\end{pmatrix}\right\} = \text{略して} \quad \{(), (123), (132)\}$$

$$S_3 = \left\{\begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\231\end{pmatrix}, \begin{pmatrix}123\\312\end{pmatrix}, \begin{pmatrix}123\\132\end{pmatrix}, \begin{pmatrix}123\\321\end{pmatrix}, \begin{pmatrix}123\\213\end{pmatrix}\right\}$$

$= \text{略して} \quad \{(), (123), (132), (23), (13), (12)\}$

例 1　$x^3 - 21x + 14 = 0$（Q上既約)のガロア群

<求め方 1＞

$D = -4 \cdot (-21)^3 - 27 \cdot 14^2 = 31752 = 2^3 \cdot 3^4 \cdot 7^2$
$\sqrt{D} = 2 \cdot 3^2 \cdot 7 \cdot \sqrt{2} = 126\sqrt{2} \notin Q$
∴ $G(L/Q) \cong S_3$

<求め方 2>

カルダノの公式（注 6）によれば
$x^3 - 21x + 14 = 0$ の解 x_1, x_2, x_3 は、
$\omega = \left(-1 + \sqrt{-3}\right)/2$　　$(\omega^3 = 1)$　として

$$x_1=\sqrt[3]{-7+\sqrt{7^2+(-7)^3}}+\sqrt[3]{-7-\sqrt{7^2+(-7)^3}}$$

$$=\sqrt[3]{-7+\sqrt{-294}}+\sqrt[3]{-7-\sqrt{-294}}$$

$$=\sqrt[3]{-7+7\sqrt{-6}}+\sqrt[3]{-7-7\sqrt{-6}}$$

$$x_2=\sqrt[3]{-7+7\sqrt{-6}}\cdot\omega+\sqrt[3]{-7-7\sqrt{-6}}\cdot\omega^2$$

$$x_3=\sqrt[3]{-7+7\sqrt{-6}}\cdot\omega^2+\sqrt[3]{-7-7\sqrt{-6}}\cdot\omega$$

（注） $\sqrt[3]{-7-7\sqrt{-6}}=\dfrac{7}{\sqrt[3]{-7+7\sqrt{-6}}}$

よって、$x^3-21x+14$ の最小分解体 $Q(x_1,x_2,x_3)=Q\left(\omega,\sqrt{-6},\sqrt[3]{-7+7\sqrt{-6}}\right)$から

それ自身への自己同型写像は、

$i:\sqrt{-6}\to\sqrt{-6},\ \sqrt[3]{-7+7\sqrt{-6}}\to\sqrt[3]{-7+7\sqrt{-6}}$
（このとき $\sqrt[3]{-7-7\sqrt{-6}}\to\sqrt[3]{-7-7\sqrt{-6}}$ ）

$\sigma:\sqrt{-6}\to\sqrt{-6},\ \sqrt[3]{-7+7\sqrt{-6}}\to\sqrt[3]{-7+7\sqrt{-6}}\cdot\omega$
（このとき $\sqrt[3]{-7-7\sqrt{-6}}\to\sqrt[3]{-7-7\sqrt{-6}}\cdot\omega^2$）

$\sigma^2:\sqrt{-6}\to\sqrt{-6},\ \sqrt[3]{-7+7\sqrt{-6}}\to\sqrt[3]{-7+7\sqrt{-6}}\cdot\omega^2$
（このとき $\sqrt[3]{-7-7\sqrt{-6}}\to\sqrt[3]{-7-7\sqrt{-6}}\cdot\omega$）

$\tau:\sqrt{-6}\to-\sqrt{-6},\ \sqrt[3]{-7+7\sqrt{-6}}\to\sqrt[3]{-7-7\sqrt{-6}}$
（このとき $\sqrt[3]{-7-7\sqrt{-6}}\to\sqrt[3]{-7+7\sqrt{-6}}$ ）

$\tau\sigma:\sqrt{-6}\to-\sqrt{-6},\ \sqrt[3]{-7+7\sqrt{-6}}\to\sqrt[3]{-7-7\sqrt{-6}}\cdot\omega$
（このとき $\sqrt[3]{-7-7\sqrt{-6}}\to\sqrt[3]{-7+7\sqrt{-6}}\cdot\omega^2$ ）

$\tau\sigma^2:\sqrt{-6}\to-\sqrt{-6},\ \sqrt[3]{-7+7\sqrt{-6}}\to\sqrt[3]{-7-7\sqrt{-6}}\cdot\omega^2$
（このとき $\sqrt[3]{-7-7\sqrt{-6}}\to\sqrt[3]{-7+7\sqrt{-6}}\cdot\omega$ ）

$$i=\begin{pmatrix}x_1x_2x_3\\x_1x_2x_3\end{pmatrix},\quad \sigma=\begin{pmatrix}x_1x_2x_3\\x_2x_3x_1\end{pmatrix},\quad \sigma^2=\begin{pmatrix}x_1x_2x_3\\x_3x_1x_2\end{pmatrix}$$

$$\tau=\begin{pmatrix}x_1x_2x_3\\x_1x_3x_2\end{pmatrix},\quad \tau\sigma=\begin{pmatrix}x_1x_2x_3\\x_3x_2x_1\end{pmatrix},\quad \tau\sigma^2=\begin{pmatrix}x_1x_2x_3\\x_2x_1x_3\end{pmatrix}$$

よって、ガロア群は、$\{i,\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\}\cong S_3$

（注 6）カルダノ($Cardano$ $1501-1576$)の公式

$x^3+px+q=0$ $(x^3=-px-q)$ の解 x_1,x_2,x_3 は、

$x=u+v$ とおくと

$x^3 = u^3 + v^3 + 3uv(u+v) = 3uvx + u^3 + v^3$

$\therefore \begin{cases} 3uv = -p \\ u^3 + v^3 = -q \end{cases}$

$\therefore \begin{cases} u^3 v^3 = (-\frac{p}{3})^3 \\ u^3 + v^3 = -q \end{cases}$

u^3とv^3 は$t^2 + qt - (\frac{p}{3})^3 = 0$ の解で

$u^3 = -\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$

$v^3 = -\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$

$u,\ v$ は $u \cdot v = -\frac{p}{3}$ となるものを選ぶとして、

$u = u$, $u\omega$, $u\omega^2$, $v = v$, $v\omega$, $v\omega^2$ より

$x_1 = u + v$

$x_2 = u\omega + v\omega^2 \ (= u\omega + v\omega^{-1})$

$x_3 = u\omega^2 + v\omega \ (= u\omega^2 + v\omega^{-2})$

<求め方 3> ガロア流

$x^3 - 21x + 14 = 0$ の解をα, β, γ とすると

$\alpha + \beta + \gamma = 0$, $\alpha\beta + \beta\gamma + \gamma\alpha = -21$, $\alpha\beta\gamma = -14$

ここで、

$V_1 = \alpha + 2\beta + 3\gamma$　　$V_2 = \alpha + 2\gamma + 3\beta$

$V_3 = \beta + 2\alpha + 3\gamma$　　$V_4 = \beta + 2\gamma + 3\alpha$

$V_5 = \gamma + 2\alpha + 3\beta$　　$V_6 = \gamma + 2\beta + 3\alpha$ とし、

$F(V) = (V - V_1)(V - V_2)(V - V_3)(V - V_4)(V - V_5)(V - V_6)$とおくと

$F(V) = V^6 - 126V^4 + 3969V^2 - 31752$　　（既約）

（#この計算などにはコンピューター を利用）

< α をV で表す>

$F(V, \alpha) = (V - (\alpha + 2\beta + 3\gamma))(V - (\alpha + 2\gamma + 3\beta))$ とし（α を固定）

$F(V, x) = (V - (x + 2\beta + 3\gamma))(V - (x + 2\gamma + 3\beta))$ とすると

$F(V, x) = 3x^2 + 3Vx + V^2 - 21$ （既約）となる。

これと $x^3 - 21x + 14 = 0$ は唯一の共通解α をもつから、

互除法の考え（注 7）を用いると、

$x^3 - 21x + 14 = 0$ を $3x^2 + 3Vx + V^2 - 21$で割った余りの

1 次式 $\left(\frac{2V^2}{3} - 14\right)x + \frac{V^3}{3} - 7V + 14$ を 0 とおいてx について解いた

ものが α である。すなわち、$\alpha = \frac{V^3-21V+42}{42-2V^2} = \frac{1}{2}\cdot\frac{V^3-21V+42}{21-V^2}$

ここで、$V(=V_1)$ において

$$0 = V^6 - 126V^4 + 3969V^2 - 31752$$

$$= (-V^4 + 105V^2 - 1764)(21 - V^2) + 5292$$

よって

$$\frac{1}{21-V^2} = \frac{1}{5292}\cdot(V^4 - 105V^2 + 1764)$$

これより、

$$\alpha = \frac{1}{2}\cdot(\frac{1}{5292})\cdot(V^3 - 21V + 42)(V^4 - 105V^2 + 1764)$$

$$= \frac{1}{10584}(V^7 - 126V^5 + 42V^4 + 3969V^3 - 4410V^2 - 37044V + 74088)$$

$$= \frac{1}{252}(V^4 - 105V^2 - 126V + 1764)$$

（注 7）ユークリッド$(Euclid\,, BC330?-275?)$の互除法

（具体例をあげて示す）

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

$g(x) = 3x^4 - 5x^3 + 5x^2 - 5x + 2\ (=0)$　は、

ただ 1 つの共通解 $x = 2/3$ をもつが、このことを

$f(x)$ と $g(x)$ の最大公約式が $(3x-2)$ であると解釈すると

次のようにユークリッドの互除法で求まる。

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

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

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

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

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

これより、最大公約式が $(3x-2)$ であり、これを 0

とおいて解いたものが共通解 $x = 2/3$ である。

＜ β をV で表す＞

$G(V,\beta) = (V - (\alpha + 2\beta + 3\gamma))(V - (\gamma + 2\beta + 3\alpha))$ とし（β を固定）

$G(V,x)=(V-(\alpha+2x+3\gamma))(V-(\gamma+2x+3\alpha))$ とすると

$G(V,x)=3x^2+V^2-84$　となる。

このあとは、α をV で表したときと同様にして

$$\beta=\frac{-42}{21-V^2}=-42\cdot\frac{1}{5292}\cdot(V^4-105V^2+1764)$$

$$=\frac{1}{252}(-2V^4+210V^2-3528)$$

< γ をV で表す>

$H(V,\gamma)=(V-(\alpha+2\beta+3\gamma))(V-(\beta+2\alpha+3\gamma))$ とし（γ を固定）

$H(V,x)=(V-(\alpha+2\beta+3x))(V-(\beta+2\alpha+3x))$ とすると

$H(V,x)=3x^2-3Vx+V^2-21$　となる。

このあとは、α をV で表したときと同様にして

$$\gamma=\frac{1}{2}\cdot\frac{-V^3+21V+42}{21-V^2}$$

$$=\frac{1}{2}\cdot\frac{1}{5292}\cdot(-V^3+21V+42)(V^4-105V^2+1764)$$

$$=\frac{1}{10584}(-V^7+126V^5+42V^4-3969V^3-4410V^2+37044V+74088)$$

$$=\frac{1}{252}(V^4-105V^2+126V+1764)$$

以上、まとめると

$$\alpha=\frac{1}{252}\left(V^4-105V^2-126V+1764\right)$$

$$\beta=\frac{1}{252}(-2V^4+210V^2-3528)$$

$$\gamma=\frac{1}{252}(V^4-105V^2+126V+1764)$$

（ただし、$V^6-126V^4+3969V^2-31752=0$ ）

これより、

$V_1=\alpha+2\beta+3\gamma\quad=V$

$V_2=\alpha+2\gamma+3\beta=\frac{1}{84}(-V^4+105V^2+42V-1764)$

$V_3=\beta+2\alpha+3\gamma=\frac{1}{84}(V^4-105V^2+42V+1764)$

$V_4=\beta+2\gamma+3\alpha=\frac{1}{84}(V^4-105V^2-42V+1764)$

$V_5=\gamma+2\alpha+3\beta=\frac{1}{84}(-V^4+105V^2-42V-1764)$

$V_6=\gamma+2\beta+3\alpha=-V$

ここで、

$$\varphi_1(x)=\frac{1}{252}\left(x^4-105x^2-126x+1764\right)$$

$$\varphi_2(x)=\frac{1}{252}(-2x^4+210x^2-3528)$$

$$\varphi_3(x)=\frac{1}{252}(x^4-105x^2+126x+1764)$$

とおくと、（$mathematica$ を利用して）

$\varphi_1(V_1)=\alpha \quad ,\varphi_2(V_1)=\beta \quad ,\varphi_3(V_1)=\gamma$

$\varphi_1(V_2)=\alpha \quad ,\varphi_2(V_2)=\gamma \quad ,\varphi_3(V_2)=\beta$

$\varphi_1(V_3)=\beta \quad ,\varphi_2(V_3)=\alpha \quad ,\varphi_3(V_3)=\gamma$

$\varphi_1(V_4)=\beta \quad ,\varphi_2(V_4)=\gamma \quad ,\varphi_3(V_4)=\alpha$

$\varphi_1(V_5)=\gamma \quad ,\varphi_2(V_5)=\alpha \quad ,\varphi_3(V_5)=\beta$

$\varphi_1(V_6)=\gamma \quad ,\varphi_2(V_6)=\beta \quad ,\varphi_3(V_6)=\alpha$

これらより

$$\begin{pmatrix}\varphi_1(V) & \varphi_2(V) & \varphi_3(V)\\ \varphi_1(V_1) & \varphi_2(V_1) & \varphi_3(V_1)\end{pmatrix}=\begin{pmatrix}\alpha & \beta & \gamma\\ \alpha & \beta & \gamma\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$$

$$\begin{pmatrix}\varphi_1(V) & \varphi_2(V) & \varphi_3(V)\\ \varphi_1(V_2) & \varphi_2(V_2) & \varphi_3(V_2)\end{pmatrix}=\begin{pmatrix}\alpha & \beta & \gamma\\ \alpha & \gamma & \beta\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

$$\begin{pmatrix}\varphi_1(V) & \varphi_2(V) & \varphi_3(V)\\ \varphi_1(V_3) & \varphi_2(V_3) & \varphi_3(V_3)\end{pmatrix}=\begin{pmatrix}\alpha & \beta & \gamma\\ \beta & \alpha & \gamma\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

$$\begin{pmatrix}\varphi_1(V) & \varphi_2(V) & \varphi_3(V)\\ \varphi_1(V_4) & \varphi_2(V_4) & \varphi_3(V_4)\end{pmatrix}=\begin{pmatrix}\alpha & \beta & \gamma\\ \beta & \gamma & \alpha\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$

$$\begin{pmatrix}\varphi_1(V) & \varphi_2(V) & \varphi_3(V)\\ \varphi_1(V_5) & \varphi_2(V_5) & \varphi_3(V_5)\end{pmatrix}=\begin{pmatrix}\alpha & \beta & \gamma\\ \gamma & \alpha & \beta\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

$$\begin{pmatrix}\varphi_1(V) & \varphi_2(V) & \varphi_3(V)\\ \varphi_1(V_6) & \varphi_2(V_6) & \varphi_3(V_6)\end{pmatrix}=\begin{pmatrix}\alpha & \beta & \gamma\\ \gamma & \beta & \alpha\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

これらガロア群は、S_3 に同型

例 2　$x^3-21x+7=0$（Q上既約)のガロア群

<求め方 1>

$D=-4\cdot(-21)^3-27\cdot 7^2=35721=3^6\cdot 7^2$

$\sqrt{D}=3^3\cdot 7=189\in Q$

$\therefore\ G(L/Q)\cong A_3$

<求め方 2>

カルダノの公式によれば

$x^3-21x+7=0$ の解 x_1,x_2,x_3 は、

$\omega=\left(-1+\sqrt{-3}\right)/2$ （$\omega^2=(-1-\sqrt{-3})/2$ ）として

$$x_1=\sqrt[3]{-\frac{7}{2}+\sqrt{(\frac{7}{2})^2+(-7)^3}}+\sqrt[3]{-\frac{7}{2}-\sqrt{(\frac{7}{2})^2+(-7)^3}}$$

$$=\sqrt[3]{-\frac{7}{2}+\frac{21}{2}\sqrt{-3}}+\sqrt[3]{-\frac{7}{2}-\frac{21}{2}\sqrt{-3}}$$

$$=\sqrt[3]{-\frac{7}{2}+\frac{21}{2}(2\omega+1)}+\sqrt[3]{-\frac{7}{2}-\frac{21}{2}(-2\omega^2-1)}$$

$$=\sqrt[3]{(21\omega+7)}+\sqrt[3]{(21\omega^2+7)}$$

$$x_2=\sqrt[3]{(21\omega+7)}\cdot\omega+\sqrt[3]{(21\omega^2+7)}\cdot\omega^2$$

$$x_3=\sqrt[3]{(21\omega+7)}\cdot\omega^2+\sqrt[3]{(21\omega^2+7)}\cdot\omega$$

（注） $\sqrt[3]{(21\omega^2+7)}=\dfrac{7}{\sqrt[3]{(21\omega+7)}}$

よって、$x^3-21x+7$ の最小分解体 $Q(x_1,x_2,x_3)=Q\left(\omega,\sqrt[3]{(21\omega+7)}\right)$から

それ自身への自己同型写像は、

i ： $\sqrt[3]{(21\omega+7)}\rightarrow\sqrt[3]{(21\omega+7)}$

σ ： $\sqrt[3]{(21\omega+7)}\rightarrow\sqrt[3]{(21\omega+7)}\cdot\omega$

（このとき、$\sqrt[3]{(21\omega^2+7)}\rightarrow\sqrt[3]{(21\omega^2+7)}\cdot\omega^2$ ）

σ^2 ： $\sqrt[3]{(21\omega+7)}\rightarrow\sqrt[3]{(21\omega+7)}\cdot\omega^2$

（このとき、$\sqrt[3]{(21\omega^2+7)}\rightarrow\sqrt[3]{(21\omega^2+7)}\cdot\omega$ ）

$$i=\begin{pmatrix}x_1x_2x_3\\x_1x_2x_3\end{pmatrix},\ \sigma=\begin{pmatrix}x_1x_2x_3\\x_2x_3x_1\end{pmatrix},\ \sigma^2=\begin{pmatrix}x_1x_2x_3\\x_3x_1x_2\end{pmatrix}$$

よって、ガロア群は、 $\{i,\sigma,\sigma^2\}\cong A_3$

<求め方 3> ガロア流（ 例 1 と同様）

$x^3-21x+7=0$ の解をα,β,γ とすると

$\alpha+\beta+\gamma=0$，　$\alpha\beta+\beta\gamma+\gamma\alpha=-21$，　$\alpha\beta\gamma=-7$

ここで、

$V_1=\alpha+2\beta+3\gamma$　　$V_2=\alpha+2\gamma+3\beta$

$V_3=\beta+2\alpha+3\gamma$　　$V_4=\beta+2\gamma+3\alpha$

$V_5=\gamma+2\alpha+3\beta$　　$V_6=\gamma+2\beta+3\alpha$ とし、

$F(V)=(V-V_1)(V-V_2)(V-V_3)(V-V_4)(V-V_5)(V-V_6)$とおくと

$F(V)=V^6-126V^4+3969V^2-35721$

$=(V^3-63V-189)(V^3-63V+189)$

（＃この計算などにはコンピューター を利用）

＜ α をV で表す＞

$F(V,\alpha)=(V-(\alpha+2\beta+3\gamma))(V-(\alpha+2\gamma+3\beta))$ とし（α を固定）

$F(V,x)=(V-(x+2\beta+3\gamma))(V-(x+2\gamma+3\beta))$ とすると

$F(V,x)=3x^2+3Vx+V^2-21$　となる

これと$x^3-21x+7=0$ は唯一の共通解 α をもつから、

互除法の考えを用いると、

$x^3-21x+7=0$ を$3x^2+3Vx+V^2-21$で割った余りの

1 次式 $\left(\frac{2V^2}{3}-14\right)x+\frac{V^3}{3}-7V+7$ を 0 とおいて x について

解いたものが α である。

すなわち、$\alpha=\frac{V^3-21V+21}{42-2V^2}=\frac{1}{2}\cdot\frac{V^3-21V+21}{21-V^2}$

ここで、$V(=V_1)$ を仮に $V^3-63V-189=0$ の解とすると(注 8)

$0=V^3-63V-189=-V(21-V^2)+(-42V-189)$

$0=V^3-63V-189=\left(-\frac{1}{42}V^2+\frac{3}{28}V+\frac{57}{56}\right)(-42V-189)+\frac{27}{8}$

これら 2 式より、

$\frac{1}{21-V^2}=-\frac{8}{27}V\left(-\frac{1}{42}V^2+\frac{3}{28}V+\frac{57}{56}\right)=-\frac{2}{63}V^2+\frac{1}{7}V+\frac{4}{3}$

これより、

$\alpha=\frac{1}{2}\cdot\frac{V^3-21V+21}{21-V^2}=\frac{1}{2}\cdot(V^3-21V+21)(-\frac{2}{63}V^2+\frac{1}{7}V+\frac{4}{3})$

$=\frac{1}{126}(-2V^5+9V^4+126V^3-231V^2-1575V+1764)$

$=-\frac{1}{3}V^2+V+14$

< β をV で表す>

$G(V,\beta)=(V-(\alpha+2\beta+3\gamma))(V-(\gamma+2\beta+3\alpha))$ とし（β を固定）

$G(V,x)=(V-(\alpha+2x+3\gamma))(V-(\gamma+2x+3\alpha))$ とすると

$G(V,x)=3x^2+V^2-84$　となる。

このあとは、α をV で表したときと同様にして

$$\beta=\frac{-21}{21-V^2}=-21\cdot(-\frac{2}{63}V^2+\frac{1}{7}V+\frac{4}{3})$$

$$=\frac{2}{3}V^2-3V-28$$

< γ をV で表す>

$H(V,\gamma)=(V-(\alpha+2\beta+3\gamma))(V-(\beta+2\alpha+3\gamma))$ とし（γ を固定）

$H(V,x)=(V-(\alpha+2\beta+3x))(V-(\beta+2\alpha+3x))$ とすると

$H(V,x)=3x^2-3Vx+V^2-21$　となる。

このあとは、α をV で表したときと同様にして

$$\gamma=\frac{1}{2}\cdot\frac{-V^3+21V+21}{21-V^2}$$

$$=\frac{1}{2}(-V^3+21V+21)(-\frac{2}{63}V^2+\frac{1}{7}V+\frac{4}{3})$$

$$=\frac{1}{126}(2V^5-9V^4-126V^3+147V^2+1953V+1764)$$

$$=-\frac{1}{3}V^2+2V+14$$

以上、まとめると

$$\alpha=-\frac{1}{3}V^2+V+14$$

$$\beta=\frac{2}{3}V^2-3V-28$$

$$\gamma=-\frac{1}{3}V^2+2V+14$$

（注意、$V^3-63V-189=0$ ）

これより、

$V_1=\alpha+2\beta+3\gamma=V$

$V_2=\alpha+2\gamma+3\beta=V^2-4V-42$

$V_3 = \beta + 2\alpha + 3\gamma = -V^2 + 5V + 42$

$V_4 = \beta + 2\gamma + 3\alpha = -V^2 + 4V + 42$

$V_5 = \gamma + 2\alpha + 3\beta = V^2 - 5V - 42$

$V_6 = \gamma + 2\beta + 3\alpha = -V$

これらの中で$V^3 - 63V - 189 = 0$ を満たすのは

$V = V_1$,V_4 ,V_5 で

$$\varphi_1(x) = -\frac{1}{3}x^2 + x + 14$$

$$\varphi_2(x) = \frac{2}{3}x^2 - 3x - 28$$

$$\varphi_3(x) = -\frac{1}{3}x^2 + 2x + 14$$

とおくと

$\varphi_1(V_1) = \alpha \quad ,\varphi_2(V_1) = \beta \quad ,\varphi_3(V_1) = \gamma$

$\varphi_1(V_4) = \beta \quad ,\varphi_2(V_4) = \gamma \quad ,\varphi_3(V_4) = \alpha$

$\varphi_1(V_5) = \gamma \quad ,\varphi_2(V_5) = \alpha \quad ,\varphi_3(V_5) = \beta$

これらより

$$\begin{pmatrix} \varphi_1(V) & \varphi_2(V) & \varphi_3(V) \\ \varphi_1(V_1) & \varphi_2(V_1) & \varphi_3(V_1) \end{pmatrix} = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha & \beta & \gamma \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} \varphi_1(V) & \varphi_2(V) & \varphi_3(V) \\ \varphi_1(V_4) & \varphi_2(V_4) & \varphi_3(V_4) \end{pmatrix} = \begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} \varphi_1(V) & \varphi_2(V) & \varphi_3(V) \\ \varphi_1(V_5) & \varphi_2(V_5) & \varphi_3(V_5) \end{pmatrix} = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

これらガロア群は、A_3 に同型。

（注意）実は、このことはV_1 ,V_4 ,V_5 の解の置換を

考えればすぐにわかることである。たとえば

V_1 で$\alpha \to \beta, \beta \to \gamma, \gamma \to \alpha$ としたものが V_4

（注 8）

$V(= V_1)$ が $V^3 - 63V - 189 = 0$ と $V^3 - 63V + 189 = 0$ の
どちらの式の解かは不明であるがどちらにしても一般性を
失わない。その式の解に$V(= V_1)$ が入っていなくても、$F(V)$
の作り方から解は $V_1 \sim V_6$ のどれかであり、α ,β ,γ の
命名を適当にやり直せば $V_1 = \alpha + 2\beta + 3\gamma$ がその式の解に
なるようにできるから。

ちなみに、$V(=V_1)$ が $V^3-63V+189=0$ の方の解とすると、

$\alpha=\frac{V^3-21V+21}{42-2V^2}=\frac{1}{2}\cdot\frac{V^3-21V+21}{21-V^2}$　　は

$0=V^3-63V+189=-V(21-V^2)+189-42V$

$0=V^3-63V+189=(189-42V)\left(\frac{57}{56}-\frac{3}{28}V-\frac{1}{42}V^2\right)+\left(-\frac{27}{8}\right)$

これら 2 式より、

$\frac{1}{21-V^2}=\frac{8}{27}V\left(\frac{57}{56}-\frac{3}{28}V-\frac{1}{42}V^2\right)$

よって、

$\alpha=\frac{1}{2}\cdot\frac{V^3-21V+21}{21-V^2}$

$=\frac{1}{2}(V^3-21V+21)\left(\frac{8}{27}V\right)\left(\frac{57}{56}-\frac{3}{28}V-\frac{1}{42}V^2\right)$

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

$=-\frac{1}{3}V^2-2V+14$

同様に考えて

$\beta=\frac{2}{3}V^2+3V-28$

$\gamma=-\frac{1}{3}V^2-V+14$

例 3　$x^3-21x+36=0$（Q上可約）のガロア群

<求め方>

$x^3-21x+36=0$ は、

$(x-3)(x^2+3x-12)=0$ となるが、

$x_1=3$ は、Q の元なので自己同型写像で不変(注 9)であり、

$x_2=(-3+\sqrt{57})/2$，　$x_3=(-3-\sqrt{57})/2$　（$=-3-x_2$）　とすれば

$x^3-21x+36=(x-3)(x-x_2)(x-x_3)$ でこれの最小分解体 L は、

$L=Q(x_2)=Q(\sqrt{57})$ でガロア群は $G=G(L/Q)=\{i\ ,\sigma\}$

ただし、$i:\sqrt{57}\to\sqrt{57}$　　，　$\sigma:\sqrt{57}\to-\sqrt{57}$

$$i=\begin{pmatrix}x_1 & x_2 & x_3\\ x_1 & x_2 & x_3\end{pmatrix}\quad,\quad \sigma=\begin{pmatrix}x_1 & x_2 & x_3\\ x_1 & x_3 & x_2\end{pmatrix}$$

これは、 S_2 に同型

（注 9）

Kを体、$\alpha\ ,\beta \in K$ とし、Kからそれ自身への自己同型写像を σ と

すると、$\sigma(0)=\sigma(0+0)=\sigma(0)+\sigma(0)$　　$\therefore\quad \sigma(0)=0$

$\sigma(1)=\sigma(1\times 1)=\sigma(1)\sigma(1)$　　$\therefore\quad \sigma(1)=1$

また、 $\alpha\ ,\beta \in K$ より、$\alpha-\beta \in K$ $,\alpha/\beta \in K$ で

$\sigma(\alpha)=\sigma(\beta+(\alpha-\beta))=\sigma(\beta)+\sigma(\alpha-\beta)$　より、

$\sigma(\alpha-\beta)=\sigma(\alpha)-\sigma(\beta)$

$\sigma(\alpha)=\sigma\left(\beta\times\frac{\alpha}{\beta}\right)=\sigma(\beta)\sigma\left(\frac{\alpha}{\beta}\right)$　より、$\sigma\left(\frac{\alpha}{\beta}\right)=\frac{\sigma(\alpha)}{\sigma(\beta)}$

これらにより、たとえば、

$\sigma(3)=\sigma(1+1+1)=\sigma(1)+\sigma(1)+\sigma(1)=1+1+1=3$

$\sigma(-3)=\sigma(0-3)=\sigma(0)-\sigma(3)=0-3=-3$

$\sigma\left(\frac{3}{5}\right)=\frac{\sigma(3)}{\sigma(5)}=\frac{3}{5}$　$,\sigma\left(-\frac{3}{5}\right)=\ \sigma\left(\frac{-3}{5}\right)=\frac{\sigma(-3)}{\sigma(5)}=\frac{-3}{5}=-\frac{3}{5}$

したがって、$a\in Q$ とすると$\sigma(a)=a$

例 4　$x^3-2x^2-x+2=0$（Q上可約）のガロア群

<求め方>

$x^3-2x^2-x+2=0$ は、

$(x+1)(x-1)(x-2)=0$ で

$x_1=-1$　，$x_2=1$ ，$x_3=2$　　とすれば

$x^3-2x^2-x+2=0$　の最小分解体 L は、

$L=Q$ でガロア群は $G=\{\,i\,\}$

ただし、$i=\begin{pmatrix}x_1x_2x_3\\x_1x_2x_3\end{pmatrix}$

これは、単位群（$\{\,i\,\}$や$\{\,e\,\}$、$(\,)$ などで表す）と同型。

4 次方程式のガロア群

4 次方程式$ax^4+bx^3+cx^2+dx+e=0$ は、$x=y-\frac{b}{4a}$ とおくことで

$y^4+sy^2+ty+u=0$ の形に書けるので、有理数体 Q 上で既約な

$x^4+px^2+qx+r=0$ の形のものを考えれば十分である。

Q 上既約な$f(x)=x^4+px^2+qx+r=0$ において、$f(x)$ の最小分解体を

$L=Q(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ とし、$f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$

$D=(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_1-\alpha_4)^2(\alpha_2-\alpha_3)^2(\alpha_2-\alpha_4)^2(\alpha_3-\alpha_4)^2$

とする。

さらに、$\theta_1=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$

$\theta_2=(\alpha_1+\alpha_3)(\alpha_2+\alpha_4)$

$\theta_3=(\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$ とすると

$\theta_1,\theta_2,\theta_3 \in L=Q(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ で

$\theta_1-\theta_2=-(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)$

$\theta_1-\theta_3=-(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)$

$\theta_2-\theta_3=-(\alpha_1-\alpha_2)(\alpha_3-\alpha_4)$

これより、

$D'=(\theta_1-\theta_2)^2(\theta_1-\theta_3)^2(\theta_2-\theta_3)^2$

$=(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_1-\alpha_4)^2(\alpha_2-\alpha_3)^2(\alpha_2-\alpha_4)^2(\alpha_3-\alpha_4)^2$

$=D$

ここで、

$g(x)=(x-\theta_1)(x-\theta_2)(x-\theta_3)$ を考えると

$\alpha_1+\alpha_2+\alpha_3+\alpha_4=0$ ，$\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4=p$

$\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4=-q$ ，$\alpha_1\alpha_2\alpha_3\alpha_4=r$　より、

$\theta_1+\theta_2+\theta_3=2p$

$\theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3=p^2-4r$

$\theta_1\theta_2\theta_3=-q^2$

よって、

$g(x)=x^3-2px^2+(p^2-4r)x+q^2$

（# これを$f(x)$ 分解多項式という）

また、

$D'=D=16p^4r-4p^3q^2-128p^2r^2+144pq^2r-27q^4+256r^3$

また、$\theta_1,\theta_2,\theta_3$ は、$\alpha_1,\alpha_2,\alpha_3,\alpha_4$ を使って書けるから

$Q \subseteq Q(\theta_1,\theta_2,\theta_3) \subseteq Q(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$

L は、Q のガロア拡大だし、$g(x)$ は、Q 上の分離多項式で、その最小分解体 $M = Q(\theta_1,\theta_2,\theta_3)$ は Q のガロア拡大。

$f(x)$ のガロア群$G = G(L/Q)$ は、S_4 の部分群と同型であって、可移群（注 1）であるから、その位数は 4 の倍数であり、24 の約数である。すなわち、24 ,12 ,8 ,4 のいずれか。

また、$G = G(L/Q) \subseteq S_4$ のうちで、$M = Q(\theta_1,\theta_2,\theta_3)$ の元 θ_1 ,θ_2 ,θ_3を不変にするもの $\sigma \in G(L/M)$としては、θ_1 ,θ_2 ,θ_3のとり方からわかるように

$V = \{(\,)\,,(12)(34)\,,(13)(24)\,,(14)(23)\,\}$（Klein の 4 元群）（注 2）

であってこのときに限る。

$\therefore$　$G(L/Q)$=$G \cap V$　（S_4 の部分群Gがいつも V を含むとは限らないから）

こうしておいて、

[1] $g(x)$ が Q 上既約であるとき

3 次方程式のガロア群のところで述べたように

$\sqrt{D'} \in Q \implies G(M/Q) \cong A_3$　（位数 3）

$\sqrt{D'} \notin Q \implies G(M/Q) \cong S_3$　（位数 6）

一方、L の Q上の拡大次数$(L/Q) = (L/M)(M/Q)$であって

$|G(L/Q)|$は、$|G(M/Q)|$の倍数

$\therefore$　$|G(L/Q)|$は、3 の倍数

また、$G(L/Q)$は可移群であって$|G(L/Q)|$は、4 の倍数

$\therefore$　$|G(L/Q)|$は、3×4=12 の倍数

$\therefore$ $G = G(L/Q) \cong A_4$ か S_4　（4 次交代群か 4 次対称群）（注 3）

このとき、$V \subset A_4$ か S_4 であって

$G(L/M)$=$G \cap V = V$

(L/M)=$|G(L/M)|$=$|V| = 4$

以上から考えると

$\sqrt{D'} = \sqrt{D} \in Q \implies G(M/Q) \cong A_3 \implies (M/Q)$=3

$\implies (L/Q)$=$(L/M)(M/Q)$=4× 3 =12

$\implies G(L/Q) \cong A_4$

$\sqrt{D'} = \sqrt{D} \notin Q \implies G(M/Q) \cong S_3 \implies (M/Q)$=6

$\implies (L/Q)$=$(L/M)(M/Q)$=4× 6 =24

$\implies G(L/Q) \cong S_4$

（注 1）G を空でない集合 X の置換群とし、Xの任意の元 x ,y に対して、$\sigma(x) = y$ を満たすG の元 σ が存在するとき Gを(X上の)可移群という。たとえば、$X = \{1\,,2\,,3\,,4\,\}$と

したとき、$G_1=\left\{\begin{pmatrix}1234\\1234\end{pmatrix},\begin{pmatrix}1234\\2143\end{pmatrix},\begin{pmatrix}1234\\3412\end{pmatrix},\begin{pmatrix}1234\\4321\end{pmatrix}\right\}$は可移群。

$G_2=\left\{\begin{pmatrix}1234\\1234\end{pmatrix},\begin{pmatrix}1234\\2143\end{pmatrix}\right\}$は置換群であるが可移群でない。

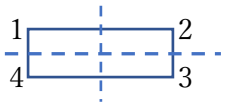
Q 上の$f(x)=0$のガロア群が可移群であれば、$f(x)$はQ 上既約である。（この逆も成り立つ+）

（注 2）この『4 次方程式のガロア群』の中では、

$()=\begin{pmatrix}1234\\1234\end{pmatrix}$,$(123)=\begin{pmatrix}1234\\2314\end{pmatrix}$,$(12)(34)=\begin{pmatrix}1234\\2143\end{pmatrix}$

$(12)=\begin{pmatrix}1234\\2134\end{pmatrix}$,$(1234)=\begin{pmatrix}1234\\2341\end{pmatrix}$ などを意味する。

$V=$長方形をそれ自身に移す対称変換



$=\{(),(12)(34),(13)(24),(14)(23)\}$

$=\left\{\begin{pmatrix}1234\\1234\end{pmatrix},\begin{pmatrix}1234\\2143\end{pmatrix},\begin{pmatrix}1234\\3412\end{pmatrix},\begin{pmatrix}1234\\4321\end{pmatrix}\right\}$

$=\{\ e\ ,\ \sigma\ ,\ \tau\ ,\ \tau\sigma\ \}$

（注意）

恒等置換は、ふつう i で表すが 4 次方程式の中では $i=\sqrt{-1}$ と混同しないように、e で表すことにする。

（注 3）

$A_4=\{\ (),(123),(124),(132),(134),(142),(143),$
$(234),(243),(12)(34),(13)(24),(14)(23)\ \}$

$S_4=\{\ A_4\ ,(12),(13),(14),(23),(24),(34),$
$(1234),(1243),(1324),(1342),(1423),(1432)\ \}$

[2] $g(x)$ が Q 上可約であるとき

① $g(x)$ が 3 つの 1 次因数の積に分解するならば、

$g(x)=(x-\theta_1)(x-\theta_2)(x-\theta_3)$ において

θ_1 ,θ_2 ,θ_3 $\in Q$ であるから

$G=G(L/Q)$=$G(L/M)$=$G\cap V$

$\therefore \quad G \subseteq V$

一方、$G \supseteq V \qquad \therefore G = V$

② $g(x)$ が 1 次と 2 次の因数の積に分解するならば

$g(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3)$ において

仮に、$\theta_1 \in Q$ ， θ_2 ，$\theta_3 \notin Q$ とすると、

$G = G(L/Q)$の元は、$\theta_1 \in Q$ を不変にする。

$\theta_1 = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$ を不変にするものは、

$V = \{(),(12)(34),(13)(24),(14)(23)\}$ のほか

(12) ，(34) ，(1324) ，(1423) の置換も合わせて

考えられ、G としては、この場合次のD_{41}とC_{41}の

2 つが考えられる。(注 4)

$D_{41} = \{V,(12),(34),(1324),(1423)\}$

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

$$\begin{pmatrix}1234\\2134\end{pmatrix},\begin{pmatrix}1234\\1243\end{pmatrix},\begin{pmatrix}1234\\3421\end{pmatrix},\begin{pmatrix}1234\\4312\end{pmatrix}\}$$

$$=\{\quad e \quad , \quad v^2 \quad , \quad \varsigma v^2 \quad , \quad \varsigma$$

$$\varsigma v^3 \quad , \quad \varsigma v \quad , \quad v^3 \quad , \quad v \quad \}$$

$$=\{e,v,v^2,v^3,\varsigma,\varsigma v,\varsigma v^2,\varsigma v^3\}$$

$C_{41} =< 1423 >$

$= \{(),(1423),(1423)^2,(1423)^3\}$

$= \{(),(1423),(12)(34),(1324)\}$

$= \{e \quad , \quad v \quad , \quad v^2 \quad , \quad v^3 \quad \}$

または、C_{41} として、

$C_{41} =< 1324 > = \{(),(1324),(1324)^2,(1324)^3\}$

$= \{(),(1324),(12)(34),(1423)\}$

$= \{e \ , \ \xi \ , \ \xi^2 \ , \ \xi^3\}$

このとき、L は、$f(x)$ の M 上の（最小）分解体でも

あることに注意すれば、

$G \cong D_{41}$(位数 8)$\Rightarrow G(L/M) = G \cap V = V$ (可移群)

$\Rightarrow G(L/M)$は可移群

$\Rightarrow f(x)$はM 上既約 （逆順も可）

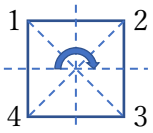
$G \cong C_{41}$(位数 4)$\Rightarrow G(L/M) = G \cap V = \{(),(12)(34)\}$ (可移群でない)

$\Rightarrow G(L/M)$は可移群でない

$\Rightarrow f(x)$はM 上可約 （逆順も可）

（注 4）実は、$D_{41} = (12)V \cup V$であって、（$\theta_2 \in Q$ ， $\theta_1, \theta_3 \notin Q$）
や（$\theta_3 \in Q$ ， $\theta_1, \theta_2 \notin Q$）を考えると、ほかに
$D_{42} = (13)V \cup V$ や $D_{43} = (14)V \cup V$がある。その場合
C_{41}に相当するものは、それぞれ、
$C_{42} =< 1234 >=< 1432 >$ ， $C_{43} =< 1342 >=< 1243 >$
である。

以下、ここでは、
$D_{41} \cong D_{42} \cong D_{43}$ なので、
D_{41} , D_{42} , D_{43}を総合して、 D_4で表す。
（D_4は位数 8 で、正 4 角形をそれ自身に移す回転変換や鏡映変換）



$C_{41} \cong C_{42} \cong C_{43}$ なので、
C_{41} , C_{42} , C_{43}を総合して、C_4 (位数 4 の巡回群)で表す。

（まとめ）

Q 上既約な$f(x)=x^4+px^2+qx+r=0$ において、

$g(x)=x^3-2px^2+(p^2-4r)x+q^2$ とし

L を $f(x)$ の最小分解体とするとき、

$D=16p^4r-4p^3q^2-128p^2r^2+144pq^2r-27q^4+256r^3$ であって

[1] $g(x)$ が Q 上既約であるとき

$\sqrt{D}\in Q \implies G(L/Q)\cong A_4$

$\sqrt{D}\notin Q \implies G(L/Q)\cong S_4$

[2] $g(x)$ が Q 上可約であるとき

① $g(x)$ が 3 つの 1 次因数の積に分解する場合

$G(L/Q)\cong V$

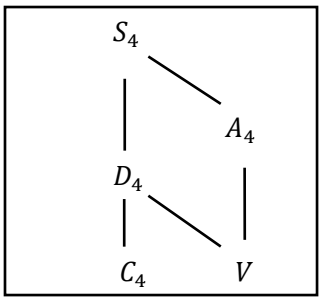
② $g(x)$ が 1 次と 2 次の因数の積に分解する場合

$g(x)$ の最小分解体をMとして、

$f(x)$がM 上既約 $\Rightarrow G(L/Q)\cong D_4$

$f(x)$がM 上可約 $\Rightarrow G(L/Q)\cong C_4$

<4 次方程式(Q 上既約)のガロア群の包含関係>



例 1　$x^4+2x^2+12x+10=0$（Q 上既約）のガロア群G

＜求め方 1＞

$x^4+px^2+qx+r=0$ の分解多項式は、

$g(x)=x^3-2px^2+(p^2-4r)x+q^2$ であったから

$g(x)=x^3-2\cdot 2\cdot x^2+(2^2-4\cdot 10)x+12^2$

$=x^3-4x^2-36x+144=(x-4)(x-6)(x+6)$

$g(x)$ が Q 上で 3 つの 1 次因数に分解されるから

ガロア群$G\cong V$

＜求め方 2＞　フェラーリの解法（注 5）で解を求めると、

$x^4=-2x^2-12x-10$

∴　$x^4+2\lambda x^2+\lambda^2=-2x^2-12x-10+2\lambda x^2+\lambda^2$

∴　$(x^2+\lambda)^2=(2\lambda-2)x^2-12x+\lambda^2-10$

右辺が完全平方式になるには、判別式＝ 0 が必要で

$(-6)^2-(2\lambda-2)(\lambda^2-10)=0$

∴　$\lambda^3-\lambda^2-10\lambda-8=0$

∴　$(\lambda+1)(\lambda+2)(\lambda-4)=0$

∴　$\lambda=-1,\lambda=-2,\lambda=4$

λ の値はどれでもよいが、λ＝ 4 とすると、

$(x^2+4)^2=6(x-1)^2$

∴　$x^2+4=\pm\sqrt{6}\,(x-1)$

∴　$x^2-\sqrt{6}\,x+4+\sqrt{6}=0$, $x^2+\sqrt{6}\,x+4-\sqrt{6}=0$

∴　$x=\frac{\sqrt{6}\pm\sqrt{-10-4\sqrt{6}}}{2}$, $x=\frac{-\sqrt{6}\pm\sqrt{-10+4\sqrt{6}}}{2}$

これより

$x_1=\frac{\sqrt{6}+\sqrt{-10-4\sqrt{6}}}{2}$, $x_2=\frac{\sqrt{6}-\sqrt{-10-4\sqrt{6}}}{2}$

$x_3=\frac{-\sqrt{6}+\sqrt{-10+4\sqrt{6}}}{2}$, $x_4=\frac{-\sqrt{6}-\sqrt{-10+4\sqrt{6}}}{2}$

（注意）$\sqrt{-10+4\sqrt{6}}=\frac{-2}{\sqrt{-10-4\sqrt{6}}}$

とおくと、

$Q(x_1,x_2,x_3,x_4)=Q(\sqrt{6},\sqrt{-10-4\sqrt{6}})$ からそれ自身への自己同型写像 は

$\sigma_0=e:\sqrt{6}\to\sqrt{6}\ ,\sqrt{-10-4\sqrt{6}}\to\sqrt{-10-4\sqrt{6}}$

（このとき、$\sqrt{-10+4\sqrt{6}}\to\sqrt{-10+4\sqrt{6}}$）

$\sigma_1=\sigma:\sqrt{6}\to\sqrt{6}\ ,\sqrt{-10-4\sqrt{6}}\to-\sqrt{-10-4\sqrt{6}}$

（このとき、$\sqrt{-10+4\sqrt{6}}\to-\sqrt{-10+4\sqrt{6}}$）

$\sigma_2=\tau:\sqrt{6}\to-\sqrt{6}\ ,\sqrt{-10-4\sqrt{6}}\to\sqrt{-10+4\sqrt{6}}$

（このとき、$\sqrt{-10+4\sqrt{6}}\to\sqrt{-10-4\sqrt{6}}$）

$\sigma_3=\tau\sigma:\sqrt{6}\to-\sqrt{6}\ ,\sqrt{-10-4\sqrt{6}}\to-\sqrt{-10+4\sqrt{6}}$

（このとき、$\sqrt{-10+4\sqrt{6}}\to-\sqrt{-10-4\sqrt{6}}$）

である。

$x_1=1\ ,x_2=2\ ,x_3=3\ ,x_4=4$ で書くと

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

これより

$G\cong\{e\ ,\sigma\ ,\tau\ ,\tau\sigma\ \}\cong V$

（注 5）フェラーリ$(Ferrari\ \ 1522-1565)$の解法

$x^4+px^2+qx+r=0$

$x^4=-px^2-qx-r$

$\therefore\ x^4+2\lambda x^2+\lambda^2=-px^2-qx-r+2\lambda x^2+\lambda^2$

$\therefore\ (x^2+\lambda)^2=(2\lambda-p)x^2-qx+\lambda^2-r$

右辺が完全平方式になるには、判別式＝0 が必要で

$(-q)^2-4(2\lambda-p)(\lambda^2-r)=0$

$\therefore\ -8\lambda^3+4p\lambda^2+8r\lambda+q^2-4pr=0$

これは、3 次方程式なのでカルダノの公式などで求まる。

そこで求めたλの値の 1 つを λ_1とすれば、与式は

$$(x^2+\lambda_1)^2=(2\lambda_1-p)\left(x-\frac{q}{4\lambda_1-2p}\right)^2$$

これより、2 つの 2 次方程式

$x^2+\lambda_1=\pm\sqrt{2\lambda_1-p}\left(x-\frac{q}{4\lambda_1-2p}\right)$ が得られ、与式の

4 つの解が求まる。

＜求め方 3＞　ガロア流

（３次方程式のガロア群 例 1 と同様だが計算量は多くなってくる）

$x^4+2x^2+12x+10=0$ の解を$\alpha,\beta,\gamma,\delta$ とすると

$\alpha+\beta+\gamma+\delta=0$,

$\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta=2$,

$\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta=-12$

$\alpha\beta\gamma\delta=10$

ここで、

$V_1=\alpha+2\beta+3\gamma+5\delta$

$V_2=\alpha+2\beta+3\delta+5\gamma$

$V_3=\alpha+2\gamma+3\beta+5\delta$

$V_4=\alpha+2\gamma+3\delta+5\beta$

……

……

$V_{23}=\delta+2\gamma+3\alpha+5\beta$

$V_{24}=\delta+2\gamma+3\beta+5\alpha$　とし、

$F(V)=(V-V_1)(V-V_2)(V-V_3)\cdots\cdots\cdots\cdots(V-V_{24})$とおくと

$=V^{24}+140V^{22}+1080V^{21}+9016V^{20}+126000V^{19}+1147880V^{18}+$

$8310960V^{17}+\cdots\cdots+6589297795500000000V+5266300910625000000$

$=(V^4+74V^2+180V+250)\times(V^4+90V^2+180V+954)\times$

$(V^4+26V^2+180V+1450)\times(V^4+50V^2+180V+2554)\times$

$(V^4-54V^2+180V+2250)\times(V^4-46V^2+180V+2650)$

（#この計算にはコンピュータ を利用）

＜ α をV で表す＞

$F(V,x)=(V-(x+2\beta+3\gamma+5\delta))(V-(x+2\beta+3\delta+5\gamma))$

$\times(V-(x+2\gamma+3\beta+5\delta))(V-(x+2\gamma+3\delta+5\beta))$

$\times\big(V-(x+2\delta+3\beta+5\gamma)\big)\big(V-(x+2\delta+3\gamma+5\beta)\big)$

とおくと、

$\beta+\gamma+\delta=-\alpha=-x$,

$\beta\gamma+\beta\delta+\gamma\delta=2-\alpha(\beta+\gamma+\delta)=2+\alpha^2=2+x^2$

$\beta\gamma\delta=-12-\alpha(\beta\gamma+\beta\delta+\gamma\delta)=-12-\alpha(2+\alpha^2)=-12-2x-x^3$

これより

$F(V,x)=1105x^6+1302Vx^5+(3428+875V^2)x^4+(11760+2800V+356V^3)x^3+$

$(2836+5040V+1232V^2+91V^4)x^2+(18816+1288V+1680V^2+288V^3+14V^5)x+$
$49680+3360V+196V^2+240V^3+28V^4+V^6$

ここで、$V=V_1$ が、仮に$V^4+74V^2+180V+250=0$ の解だとすると(注 6)

$F(V,x)=\ 1105x^6+1302Vx^5+(3428+875V^2)x^4+(11760+2800V+356V^3)x^3$
$+(-19914-11340V-5502V^2)x^2+(18816-2212V-840V^2-748V^3)x$
$+61180+11640V+3350V^2+60V^3$

となり、これと

$x^4+2x^2+12x+10$ は唯一の共通解 α をもつから、互除法の考えで割り算を繰り返すと最後に 1 次式 $Ax+B$で割るところまで進むがこれを 0 とおいて、$x(=\alpha)=-B/A$ が求まる。

（計算式は、非常に長くなるので省略する）

$\alpha=(-7190+347\mathrm{V}-260V^2+18V^3)/6095$

同様にして、

$\beta=(-2980-9047\mathrm{V}+350V^2-118V^3)/6095$

$\gamma=(18850+9829\mathrm{V}-5V^2+141V^3)/6095$

$\delta=(-8680-1129\mathrm{V}-85V^2-41V^3)/6095$

（ただし、$V^4+74V^2+180V+250=0$ ）

これより、

$V_1=\alpha+2\beta+3\gamma+5\delta=V$

$V_2=\alpha+2\beta+3\delta+5\gamma=(55060+28011V+160V^2+364V^3)/6095$

……

$V_8=\beta+2\alpha+3\delta+5\gamma=(10170+7481V-90V^2+100V^3)/1219$

……

$V_{17}=\gamma+2\delta+3\alpha+5\beta=(-660-691V+15V^2-9V^3)/115$

……

$V_{24}=\delta+2\gamma+3\beta+5\alpha=(-690-299\mathrm{V}-15V^2-V^3)/265$

これらの中で、$V^4+74V^2+180V+250=0$を満たすのは、

V_1 ,V_8 ,V_{17} ,V_{24} である。

ここで、

$\varphi_1(x)=(-7190+347x-260x^2+18x^3)/6095$

$\varphi_2(x)=(-2980-9047x+350x^2-118x^3)/6095$

$\varphi_3(x)=(18850+9829x-5x^2+141x^3)/6095$

$\varphi_4(x)=(-8680-1129x-85x^2-41x^3)/6095$

とおくと

$\varphi_1(V_1)=\ \alpha\ ,\varphi_2(V_1)=\beta\ \ ,\varphi_3(V_1)=\gamma\ ,\varphi_4(V_1)=\delta$

$\varphi_1(V_8) = \beta\ ,\varphi_2(V_8) = \alpha\ \ ,\varphi_3(V_8) = \delta\ ,\varphi_4(V_8) = \gamma$

$\varphi_1(V_{17}) = \gamma\ ,\varphi_2(V_{17}) = \delta\ \ ,\varphi_3(V_{17}) = \alpha\ ,\varphi_4(V_{17}) = \beta$

$\varphi_1(V_{24}) = \delta\ ,\varphi_2(V_{24}) = \gamma\ \ ,\varphi_3(V_{24}) = \beta\ ,\varphi_4(V_{24}) = \alpha$

これらより

$$\begin{pmatrix} \varphi_1(V)\ ,\varphi_2(V)\ ,\varphi_3(V)\ ,\varphi_4(V) \\ \varphi_1(V_1)\ ,\varphi_2(V_1)\ ,\varphi_3(V_1)\ ,\varphi_4(V_1) \end{pmatrix}=\begin{pmatrix}\alpha\beta\gamma\delta\\ \alpha\beta\gamma\delta\end{pmatrix} = \begin{pmatrix}1234\\1234\end{pmatrix}$$

$$\begin{pmatrix} \varphi_1(V)\,,\varphi_2(V)\,,\varphi_3(V)\,,\varphi_4(V) \\ \varphi_1(V_8),\varphi_2(V_8),\varphi_3(V_8),\varphi_4(V_8) \end{pmatrix}=\begin{pmatrix}\alpha\beta\gamma\delta\\ \beta\alpha\delta\gamma\end{pmatrix} = \begin{pmatrix}1234\\2143\end{pmatrix}$$

$$\begin{pmatrix} \varphi_1(V)\,,\varphi_2(V)\,,\varphi_3(V)\,,\varphi_4(V) \\ \varphi_1(V_{17}),\varphi_2(V_{17}),\varphi_3(V_{17}),\varphi_4(V_{17}) \end{pmatrix}=\begin{pmatrix}\alpha\beta\gamma\delta\\ \gamma\delta\alpha\beta\end{pmatrix} = \begin{pmatrix}1234\\3412\end{pmatrix}$$

$$\begin{pmatrix} \varphi_1(V)\,,\varphi_2(V)\,,\varphi_3(V)\,,\varphi_4(V) \\ \varphi_1(V_{24}),\varphi_2(V_{24}),\varphi_3(V_{24}),\varphi_4(V_{24}) \end{pmatrix}=\begin{pmatrix}\alpha\beta\gamma\delta\\ \delta\gamma\beta\alpha\end{pmatrix} = \begin{pmatrix}1234\\4321\end{pmatrix}$$

これより、

$$G \cong \left\{ \begin{pmatrix}1234\\1234\end{pmatrix}\ \begin{pmatrix}1234\\2143\end{pmatrix}\ \begin{pmatrix}1234\\3412\end{pmatrix}\ \begin{pmatrix}1234\\4321\end{pmatrix}\right\} \cong V$$

（注意） 実はこのことは、$V_1\ ,V_8\ ,V_{17}\ ,V_{24}$ の解の置換を
考えればすぐにわかる。
たとえば、V_1 とV_{17} とでは、α とγ を入れ換え
β とδ を入れ換えたものになっている。

（注 6）（3 次方程式のガロア群のところでやったように）

$V(=V_1)$が$V^4+74V^2+180V+250=0\ ,V^4+90V^2+180V+954=0$

$V^4+26V^2+180V+1450=0\ \ ,V^4+50V^2+180V+2554=0$

$V^4-54V^2+180V+2250=0\ ,\quad V^4-46V^2+180V+2650=0$

のどの式の解かは不明であるがどれにしても一般性を失わない。

その式の解に$V(=V_1)$ が入っていなくても、$F(V)$ の作り方から解は

$V_1 \sim V_{24}$ のどれかであり、$\alpha\ ,\beta\ ,\gamma\ ,\delta$ の命名を適当にやり直せば

$V_1=\alpha+2\beta+3\gamma+5\delta$ がその式の解になるようにできるから。

例 2　$x^4+2x^2+8x+11=0$（Q 上既約）のガロア群G

＜求め方 1＞

分解多項式は、

$g(x)=x^3-2\cdot2\cdot x^2+(2^2-4\cdot11)x+8^2$

$\quad=x^3-4x^2-40x+64\ =(x-8)(x^2+4x-8)$

$g(x)$ が Q 上で 1 次と 2 次の因数の積に分解される。

一方、$g(x)$ の最小分解体は、$M=Q(\sqrt{3})$ であって

$x^4+2x^2+8x+11$ は、$M=Q(\sqrt{3})$ 上既約である。

∴　ガロア群$G \cong D_4$

<求め方２>　フェラーリの解法で解を求めると、

$x^4=-2x^2-8x-11$

∴ $x^4+2\lambda x^2+\lambda^2=-2x^2-8x-11+2\lambda x^2+\lambda^2$

∴ $(x^2+\lambda)^2=(2\lambda-2)x^2-8x+\lambda^2-11$

右辺が完全平方式になるには、判別式＝０が必要で

$(-4)^2-(2\lambda-2)(\lambda^2-11)=0$

∴ $\lambda^3-\lambda^2-11\lambda+3=0$

∴ $(\lambda+3)(\lambda^2-4\lambda+1)=0$

∴ $\lambda=-3\,,\lambda=2\pm\sqrt{3}$

λの値はどれでもよいが、$\lambda=2+\sqrt{3}$ とすると、

$$(x^2+2+\sqrt{3})^2=(2+2\sqrt{3})(x-\frac{4}{2+2\sqrt{3}})^2$$

$$x^2+2+\sqrt{3}=\pm\sqrt{2+2\sqrt{3}}\,(x-\frac{4}{2+2\sqrt{3}})$$

$$x^2-\sqrt{2+2\sqrt{3}}\cdot x+2+\sqrt{3}+\frac{4}{\sqrt{2+2\sqrt{3}}}=0$$

$$x^2+\sqrt{2+2\sqrt{3}}\cdot x+2+\sqrt{3}-\frac{4}{\sqrt{2+2\sqrt{3}}}=0$$

これらより

$$x_1=\frac{\sqrt{2+2\sqrt{3}}+\sqrt{-6-2\sqrt{3}-\frac{16}{\sqrt{2+2\sqrt{3}}}}}{2}$$

$$\left(\quad=\frac{\sqrt{2+2\sqrt{3}}+\sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}}{2}\quad\right)$$

$$x_2=\frac{\sqrt{2+2\sqrt{3}}-\sqrt{-6-2\sqrt{3}-\frac{16}{\sqrt{2+2\sqrt{3}}}}}{2}$$

$$x_3=\frac{-\sqrt{2+2\sqrt{3}}+\sqrt{-6-2\sqrt{3}+\frac{16}{\sqrt{2+2\sqrt{3}}}}}{2}$$

$$x_4 = \frac{-\sqrt{2+2\sqrt{3}} - \sqrt{-6-2\sqrt{3}+\dfrac{16}{\sqrt{2+2\sqrt{3}}}}}{2}$$

とおくと、

（注意）　$\sqrt{-6-2\sqrt{3}+\frac{16}{\sqrt{2+2\sqrt{3}}}} = \frac{-2\sqrt{28-10\sqrt{3}}}{\sqrt{-6-2\sqrt{3}-\frac{16}{\sqrt{2+2\sqrt{3}}}}}$

$$Q(x_1,x_2,x_3,x_4) = Q\left(\sqrt{2+2\sqrt{3}}, \sqrt{-6-2\sqrt{3}-\frac{16}{\sqrt{2+2\sqrt{3}}}}, \sqrt{-6-2\sqrt{3}+\frac{16}{\sqrt{2+2\sqrt{3}}}}\right)$$

$$= Q\left(\sqrt{2+2\sqrt{3}}, \sqrt{28-10\sqrt{3}}, \sqrt{-6-2\sqrt{3}-\frac{16}{\sqrt{2+2\sqrt{3}}}}\right)$$

$$\left(= Q\left(\sqrt{2+2\sqrt{3}}, \sqrt{28-10\sqrt{3}}, \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}\right) \right)$$

からそれ自身への自己同型写像 は

$\sigma_0 = e$:
$$\sqrt{2+2\sqrt{3}} \to \sqrt{2+2\sqrt{3}}, \sqrt{28-10\sqrt{3}} \to \sqrt{28-10\sqrt{3}}$$
$$, \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}} \to \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}$$

$\sigma_1 = \sigma$:
$$\sqrt{2+2\sqrt{3}} \to \sqrt{2+2\sqrt{3}}, \sqrt{28-10\sqrt{3}} \to -\sqrt{28-10\sqrt{3}}$$
$$, \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}} \to \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}$$

$\sigma_2 = \tau$:
$$\sqrt{2+2\sqrt{3}} \to \sqrt{2+2\sqrt{3}}, \sqrt{28-10\sqrt{3}} \to \sqrt{28-10\sqrt{3}}$$
$$, \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}} \to -\sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}$$

$\sigma_3 = \tau\sigma$:
$$\sqrt{2+2\sqrt{3}} \to \sqrt{2+2\sqrt{3}}, \sqrt{28-10\sqrt{3}} \to -\sqrt{28-10\sqrt{3}}$$
$$, \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}} \to -\sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}$$

$\sigma_4 = \xi$:
$$\sqrt{2+2\sqrt{3}} \to -\sqrt{2+2\sqrt{3}}, \sqrt{28-10\sqrt{3}} \to \sqrt{28-10\sqrt{3}}$$
$$, \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}} \to \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}$$

$\sigma_5 = \sigma\xi$: $\sqrt{2+2\sqrt{3}} \to -\sqrt{2+2\sqrt{3}}$, $\sqrt{28-10\sqrt{3}} \to -\sqrt{28-10\sqrt{3}}$

, $\sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}} \to \sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}$

$\sigma_6 = \tau\xi$: $\sqrt{2+2\sqrt{3}} \to -\sqrt{2+2\sqrt{3}}$, $\sqrt{28-10\sqrt{3}} \to \sqrt{28-10\sqrt{3}}$

, $\sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}} \to -\sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}$

$\sigma_7 = \tau\sigma\xi$: $\sqrt{2+2\sqrt{3}} \to -\sqrt{2+2\sqrt{3}}$, $\sqrt{28-10\sqrt{3}} \to -\sqrt{28-10\sqrt{3}}$

, $\sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}} \to -\sqrt{-6-2\sqrt{3}-8\sqrt{-1+\sqrt{3}}}$

$x_1 = 1$, $x_2 = 2$, $x_3 = 3$, $x_4 = 4$ で書くと

$e = \begin{pmatrix}1234\\1234\end{pmatrix}$, $\sigma = \begin{pmatrix}1234\\1243\end{pmatrix}$, $\tau = \begin{pmatrix}1234\\2143\end{pmatrix}$, $\tau\sigma = \begin{pmatrix}1234\\2134\end{pmatrix}$

$\xi = \begin{pmatrix}1234\\3412\end{pmatrix}$, $\sigma\xi = \begin{pmatrix}1234\\4312\end{pmatrix}$, $\tau\xi = \begin{pmatrix}1234\\4321\end{pmatrix}$, $\tau\sigma\xi = \begin{pmatrix}1234\\3421\end{pmatrix}$

ここで、改めて、, $\tau\sigma\xi = \begin{pmatrix}1234\\3421\end{pmatrix} = \upsilon$, $\sigma = \begin{pmatrix}1234\\1243\end{pmatrix} = \eta$ と書き直すと

これらは、

$e = \begin{pmatrix}1234\\1234\end{pmatrix}$, $\upsilon = \begin{pmatrix}1234\\3421\end{pmatrix}$, $\upsilon^2 = \begin{pmatrix}1234\\2143\end{pmatrix}$, $\upsilon^3 = \begin{pmatrix}1234\\4312\end{pmatrix}$

$\eta = \begin{pmatrix}1234\\1243\end{pmatrix}$, $\eta\upsilon = \begin{pmatrix}1234\\4321\end{pmatrix}$, $\eta\upsilon^2 = \begin{pmatrix}1234\\2134\end{pmatrix}$, $\eta\upsilon^3 = \begin{pmatrix}1234\\3412\end{pmatrix}$

これより

$G \cong \{e, \upsilon, \upsilon^2, \upsilon^3, \eta, \eta\upsilon, \eta\upsilon^2, \eta\upsilon^3\} \cong D_4$

<求め方 3> ガロア流

例 1 と全く同様だが、計算式の値が大きくて

コンピューターを利用しても大変である。

以後は、この求め方は中止。

$x^4 + 2x^2 + 8x + 11 = 0$ の解を$\alpha, \beta, \gamma, \delta$ とすると

$\alpha+\beta+\gamma+\delta=0$,

$\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta=2$,

$\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta=-8$

$\alpha\beta\gamma\delta=11$

ここで、

$V_1=\alpha+2\beta+3\gamma+5\delta$

$V_2=\alpha+2\beta+3\delta+5\gamma$

……

$V_6=\alpha+2\delta+3\gamma+5\beta$

……

$V_8=\beta+2\alpha+3\delta+5\gamma$

……

$V_{10}=\beta+2\gamma+3\delta+5\alpha$

……

$V_{15}=\gamma+2\beta+3\alpha+5\delta$

……

$V_{17}=\gamma+2\delta+3\alpha+5\beta$

……

$V_{19}=\delta+2\alpha+3\beta+5\gamma$

……

$V_{24}=\delta+2\gamma+3\beta+5\alpha$　とし、

$F(V)=(V-V_1)(V-V_2)(V-V_3)\cdots\cdots\cdots\cdots(V-V_{24})$とおくと

$F(V)=V^{24}+140V^{22}+720V^{21}+9086V^{20}+84000V^{19}+\cdots\cdots$

……

$+3403502053814404080V+2757331011778954281$

$=(V^8+20V^6+240V^5+1258V^4+2400V^3+150396V^2+346320V+421641)$

$\times(V^8-60V^6+240V^5+2138V^4-7200V^3-16596V^2+240720V+728761)$

$\times(V^8+180V^6+240V^5+14090V^4+21600V^3+591900V^2+741840V+8973481)$

（#この計算にはコンピュータ－ を利用）

＜ α をV で表す>

$F(V,x)=(V-(x+2\beta+3\gamma+5\delta))(V-(x+2\beta+3\delta+5\gamma))$

$\times(V-(x+2\gamma+3\beta+5\delta))(V-(x+2\gamma+3\delta+5\beta))$

$\times\big(V-(x+2\delta+3\beta+5\gamma)\big)\big(V-(x+2\delta+3\gamma+5\beta)\big)$

とおくと、

$\beta+\gamma+\delta=-\alpha=-x$,

$\beta\gamma+\beta\delta+\gamma\delta=2-\alpha(\beta+\gamma+\delta)=2+\alpha^2=2+x^2$

$\beta\gamma\delta=-8-\alpha(\beta\gamma+\beta\delta+\gamma\delta)=-8-x(2+x^2)=-x^3-2x-8$

これより

$F(V,x)=1105x^6+414Vx^5+(4052+35V^2)x^4+(24400+1880V+28V^3)x^3$

$+(4324+5040V+392V^2+19V^4)x^2$

$+(42016+1976V-560V^2+24V^3-2V^5)x$

$+141760+14560V+676V^2+560V^3+52V^4+V^6$

(#この計算にはコンピュータ を利用)

ここで、$V=V_1$ が仮に

$V^8+20V^6+240V^5+1258V^4+2400V^3+150396V^2+346320V+421641=0$ の

解だとすると、 $F(V,x)$と $x^4+2x^2+8x+11$ は唯一の共通解 α を

もつから、互除法の考えで、割り算を繰り返すと最後に 1 次式 $Ax+B$で

割るところまで進むが これを 0 とおいて、$x(=\alpha)=-B/A$

が求まる。(コンピュータを利用しないと無理)

すなわち、

$$\alpha=-\frac{2111884733989}{1090512378241}-\frac{1291608557585 79V}{191930178570416}-\frac{1081249050951V^2}{95965089285208}-\frac{3934830999173V^3}{575790535711248}$$

$$-\frac{29122965935V^4}{47982544642604}-\frac{25276831669V^5}{575790535711248}-\frac{983717601V^6}{95965089285208}-\frac{1766788733V^7}{575790535711248}$$

同様にして

$$\beta=\frac{3367087226831}{1090512378241}+\frac{482174117256971V}{287895267855624}+\frac{1177445721057V^2}{47982544642604}+\frac{13914914049077V^3}{863685803566872}+$$

$$\frac{164087081705V^4}{71973816963906}+\frac{225672953221V^5}{863685803566872}-\frac{376674179V^6}{143947633927812}+\frac{9564473837V^7}{863685803566872}$$

$$\gamma=-\frac{1653722744537}{2181024756482}-\frac{319817495025021V}{191930178570416}-\frac{1369839061269V^2}{95965089285208}-\frac{6045252050731V^3}{575790535711248}-$$

$$\frac{105841149835V^4}{47982544642604}-\frac{175119289883V^5}{575790535711248}+\frac{2344109381V^6}{95965089285208}-\frac{6030896371V^7}{575790535711248}$$

$$\delta=-\frac{856682241147}{2181024756482}+\frac{191293408918429V}{287895267855624}+\frac{48098335053V^2}{47982544642604}+\frac{1055210525779V^3}{863685803566872}$$

$$+\frac{19179545975V^4}{35986908481953}+\frac{74921229107V^5}{863685803566872}-\frac{1663913491V^6}{143947633927812}+\frac{2132053819V^7}{863685803566872}$$

(注意、$V^8+20V^6+240V^5+1258V^4+2400V^3+150396V^2+346320V+421641=0$)

これより、

$V_1 = \alpha + 2\beta + 3\gamma + 5\delta = V$

……

$V_6 = \alpha + 2\delta + 3\gamma + 5\beta = \frac{22772570084427}{2181024756482} + \frac{193422898811875V}{47982544642604} +$

$\frac{847010539503V^2}{11995636160651} + \frac{6429851761649V^3}{143947633927812} +$

$\frac{125727989755V^4}{23991272321302} + \frac{75375862057V^5}{143947633927812} +$

$\frac{321809828V^6}{11995636160651} + \frac{3716210009V^7}{143947633927812}$

……

$V_8 = \beta + 2\alpha + 3\delta + 5\gamma =$　省略

……

$V_{10} = \beta + 2\gamma + 3\delta + 5\alpha =$　省略

……

$V_{15} = \gamma + 2\beta + 3\alpha + 5\delta =$　省略

……

$V_{17} = \gamma + 2\delta + 3\alpha + 5\beta =$　省略

……

$V_{19} = \delta + 2\alpha + 3\beta + 5\gamma =$　省略

……

$V_{24} = \delta + 2\gamma + 3\beta + 5\alpha = -\frac{5504281375}{2362973734} - \frac{629129236349V}{623825065776} -$

$-\frac{1067229015V^2}{103970844296} - \frac{10502786507V^3}{1871475197328} -$

$-\frac{11539235V^4}{155956266444} + \frac{80186309V^5}{1871475197328} -$

$\frac{6802795V^6}{311912532888} - \frac{1122707V^7}{1871475197328}$

これら V_1 ～ V_{24} の中で、

$V^8 + 20V^6 + 240V^5 + 1258V^4 + 2400V^3 + 150396V^2 + 346320V + 421641 = 0$ を

満たすのは、 V_1 ,V_6 ,V_8 ,V_{10} ,V_{15} ,V_{17} ,V_{19} ,V_{24} である。

これより、(例 1 と同様に進めて)

……

(途中省略するが、これらの解の置換をみれば)

・・・・・・・・・・・・・

ガロア群G としては、

$\begin{pmatrix}\alpha\beta\gamma\delta\\ \alpha\beta\gamma\delta\end{pmatrix}=\begin{pmatrix}1234\\ 1234\end{pmatrix}$，$\begin{pmatrix}\alpha\beta\gamma\delta\\ \alpha\delta\gamma\beta\end{pmatrix}=\begin{pmatrix}1234\\ 1432\end{pmatrix}$，$\begin{pmatrix}\alpha\beta\gamma\delta\\ \beta\alpha\delta\gamma\end{pmatrix}=\begin{pmatrix}1234\\ 2143\end{pmatrix}$，$\begin{pmatrix}\alpha\beta\gamma\delta\\ \beta\gamma\delta\alpha\end{pmatrix}=\begin{pmatrix}1234\\ 2341\end{pmatrix}$

$\begin{pmatrix}\alpha\beta\gamma\delta\\ \gamma\beta\alpha\delta\end{pmatrix}=\begin{pmatrix}1234\\ 3214\end{pmatrix}$，$\begin{pmatrix}\alpha\beta\gamma\delta\\ \gamma\delta\alpha\beta\end{pmatrix}=\begin{pmatrix}1234\\ 3412\end{pmatrix}$，$\begin{pmatrix}\alpha\beta\gamma\delta\\ \delta\alpha\beta\gamma\end{pmatrix}=\begin{pmatrix}1234\\ 4123\end{pmatrix}$，$\begin{pmatrix}\alpha\beta\gamma\delta\\ \delta\gamma\beta\alpha\end{pmatrix}=\begin{pmatrix}1234\\ 4321\end{pmatrix}$

ここで、

$\begin{pmatrix}1234\\ 2341\end{pmatrix}=\nu$ ，$\begin{pmatrix}1234\\ 3214\end{pmatrix}=\xi$ とおくと、

$\nu^2=\begin{pmatrix}1234\\ 3412\end{pmatrix}$ ，$\nu^3=\begin{pmatrix}1234\\ 4123\end{pmatrix}$

$\xi\nu=\begin{pmatrix}1234\\ 2143\end{pmatrix}$ ，　$\xi\nu^2=\begin{pmatrix}1234\\ 1432\end{pmatrix}$ ，　$\xi\nu^3=\begin{pmatrix}1234\\ 4321\end{pmatrix}$

これらは、

$\{e\ ,\nu\ ,\nu^2,\nu^3,\xi\ ,\xi\nu,\xi\nu^2,\xi\nu^3\ \}$

これより、 ガロア群$G\cong D_4$

例 3　$x^4+2x^2+8x+9=0$（Q 上既約)のガロア群G

<求め方 1>

分解多項式は、

$g(x)=x^3-2\cdot2\cdot x^2+(2^2-4\cdot9)x+8^2$

$=x^3-4x^2-32x+64$　（Q 上既約）

$x=y+\frac{4}{3}$で変換すると

$h(y)=y^3-\frac{112}{3}y+\frac{448}{27}$　（Q 上既約）

$g(x)=0$ の解を $\alpha,\ \beta,\ \gamma$ とすれば、$h(y)=0$ の解は

$\alpha-\frac{4}{3},\ \beta-\frac{4}{3},\ \gamma-\frac{4}{3}$ である。

$g(x)=0$ の判別式をD'，$h(y)=0$ の判別式をD'' とすれば、

$D''=(\left(\alpha-\frac{4}{3}\right)-\left(\beta-\frac{4}{3}\right))^2(\left(\alpha-\frac{4}{3}\right)-\left(\gamma-\frac{4}{3}\right))^2(\left(\beta-\frac{4}{3}\right)-\left(\gamma-\frac{4}{3}\right))^2$

$=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$

$=D'$

$=-4\cdot\left(-\frac{112}{3}\right)^3-27\cdot\left(\frac{448}{27}\right)^2=2^{12}\cdot7^2$

$\therefore\ \sqrt{D'}=2^6\cdot7=448\in Q$

$\therefore\ \ G\cong A_4$

＜求め方 2＞　フェラーリの解法で解を求めると、

$$x^4 = -2x^2 - 8x - 9$$

$$\therefore \quad x^4 + 2\lambda x^2 + \lambda^2 = -2x^2 - 8x - 9 + 2\lambda x^2 + \lambda^2$$

$$\therefore \quad (x^2 + \lambda)^2 = (2\lambda - 2)x^2 - 8x + \lambda^2 - 9$$

右辺が完全平方式になるには、判別式＝0 が必要で

$$(-4)^2 - (2\lambda - 2)(\lambda^2 - 9) = 0$$

$$\therefore \quad \lambda^3 - \lambda^2 - 9\lambda + 1 = 0$$

$\lambda = m + \frac{1}{3}$ とおくと、

$$m^3 - \frac{28}{3}m - \frac{56}{27} = 0$$

(これはガロア群 A_3 をもつ)

カルダノの公式より、解の 1 つは、

$$m = \sqrt[3]{\frac{28}{27} + \sqrt{\left(-\frac{28}{27}\right)^2 + \left(-\frac{28}{9}\right)^3}} + \sqrt[3]{\frac{28}{27} - \sqrt{\left(-\frac{28}{27}\right)^2 + \left(-\frac{28}{9}\right)^3}}$$

$$= \sqrt[3]{\frac{28}{27} + \frac{28}{9}\sqrt{-3}} + \sqrt[3]{\frac{28}{27} - \frac{28}{9}\sqrt{-3}}$$

$\omega = (-1 + \sqrt{-3})/2$ とおくと $\omega^2 = (-1 - \sqrt{-3})/2$ で

$$m = \frac{1}{3}(\sqrt[3]{112 + 168\omega} + \sqrt[3]{112 + 168\omega^2})$$

$$\therefore \quad \lambda = \frac{1}{3}(\,1 + \sqrt[3]{112 + 168\omega} + \sqrt[3]{112 + 168\omega^2}\,)$$

（ 注意：$\sqrt[3]{112 + 168\omega^2} = \frac{28}{\sqrt[3]{112+168\omega}}$ ）

このとき、

$$(x^2 + \lambda)^2 = (2\lambda - 2)(x - \frac{4}{2\lambda - 2})^2$$

$$\therefore \quad x^2 + \lambda = \pm\sqrt{2\lambda - 2}\left(x - \frac{4}{2\lambda - 2}\right)$$

$$\therefore \quad x^2 + \lambda = \sqrt{2\lambda - 2}\,x - \frac{4}{\sqrt{2\lambda-2}} \ , \ x^2 + \lambda = -\sqrt{2\lambda - 2}\,x + \frac{4}{\sqrt{2\lambda-2}}$$

$$\therefore\ x^2 - \sqrt{2\lambda - 2}\ x + \lambda + \frac{4}{\sqrt{2\lambda - 2}} = 0\ ,\ x^2 + \sqrt{2\lambda - 2}\ x + \lambda - \frac{4}{\sqrt{2\lambda - 2}} = 0$$

これらより、

$$\therefore\quad x_1=\frac{(\lambda-1)+\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}}{\sqrt{2\lambda-2}}$$

$$x_2=\frac{(\lambda-1)-\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}}{\sqrt{2\lambda-2}}$$

$$x_3=\frac{-(\lambda-1)+\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}}{\sqrt{2\lambda-2}}$$

$$x_4=\frac{-(\lambda-1)-\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}}{\sqrt{2\lambda-2}}$$

（注意：$\lambda^3-\lambda^2-9\lambda+1=0$ より

$\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}=\frac{\sqrt{\lambda^4-2\lambda^2-32\lambda+33}}{\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}}=\frac{\sqrt{8(\lambda^2-3\lambda+4)}}{\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}}$ ）

これより、$\lambda=\frac{1}{3}(1+\sqrt[3]{112+168\omega}+\sqrt[3]{112+168\omega^2})$ として

$Q(x_1,x_2,x_3,x_4)=Q(\omega,\sqrt[3]{112+168\omega},\sqrt{2\lambda-2},\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}},\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}})$

$=Q(\omega,\sqrt[3]{112+168\omega},\sqrt{2\lambda-2},\sqrt{8(\lambda^2-3\lambda+4)},\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}})$

からそれ自身への自己同型写像σは、以下のA群 $\{a_1,a_2,a_3\}$とB群 $\{b_1,b_2,b_3,b_4\}$の組み合わせより、$3\times4=12$通り考えられ、ガロア群$G\cong A_4$（？）

A群

a_1 ： $\sqrt[3]{112+168\omega}\ \to\sqrt[3]{112+168\omega}$

（このとき、$\sqrt[3]{112+168\omega^2}\ \to\ \sqrt[3]{112+168\omega^2}$ ）

a_2 ： $\sqrt[3]{112+168\omega}\ \to\ \sqrt[3]{112+168\omega}\cdot\omega$

（このとき、$\sqrt[3]{112+168\omega^2}\ \to\ \sqrt[3]{112+168\omega^2}\cdot\omega^2$ ）

a_3 ： $\sqrt[3]{112+168\omega}\ \to\ \sqrt[3]{112+168\omega}\cdot\omega^2$

（このとき、$\sqrt[3]{112+168\omega^2}\ \to\ \sqrt[3]{112+168\omega^2}\cdot\omega$ ）

B群 （ $\lambda=\frac{1}{3}\left(1+\sqrt[3]{112+168\omega}+\sqrt[3]{112+168\omega^2}\right)$ として ）

b_1 ： $\sqrt{8\left(\lambda^2-3\lambda+4\right)}\ \to\sqrt{8\left(\lambda^2-3\lambda+4\right)}$

，$\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}\ \to\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}$

（このとき，$\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}\ \to\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}$ ）

b_2 ： $\sqrt{8(\lambda^2-3\lambda+4)}\ \to\ -\sqrt{8(\lambda^2-3\lambda+4)}$

，$\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}\ \to\ \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}$

（このとき，$\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}\ \to-\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}$ ）

b_3 ： $\sqrt{8(\lambda^2-3\lambda+4)}\ \to\sqrt{8(\lambda^2-3\lambda+4)}$

$, \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}} \rightarrow -\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}$

（このとき，$\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}} \rightarrow -\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}$ ）

b_4 ： $\sqrt{8\left(\lambda^2-3\lambda+4\right)} \rightarrow -\sqrt{8\left(\lambda^2-3\lambda+4\right)}$

$, \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}} \rightarrow -\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}$

（このとき，$\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}} \rightarrow \sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}$ ）

例 4　$x^4+2x^2+8x+16=0$（Q 上既約)のガロア群G

<求め方 1>

分解多項式は、

$g(x)=x^3-2\cdot 2\cdot x^2+(2^2-4\cdot 16)x+8^2$

$=x^3-4x^2-60x+64$　　（Q 上既約）

$x=y+\frac{4}{3}$ で変換すると

$h(y)=y^3-\frac{196}{3}y-\frac{560}{27}$　（Q 上既約）

$g(x)=0$ の解を $\alpha,\ \beta,\ \gamma$ とすれば、$h(y)=0$ の解は

$\alpha-\frac{4}{3},\ \beta-\frac{4}{3},\ \gamma-\frac{4}{3}$ である。

$g(x)=0$ の判別式をD'，$h(y)=0$ の判別式をD'' とすれば、

$D''=(\left(\alpha-\frac{4}{3}\right)-\left(\beta-\frac{4}{3}\right))^2(\left(\alpha-\frac{4}{3}\right)-\left(\gamma-\frac{4}{3}\right))^2(\left(\beta-\frac{4}{3}\right)-\left(\gamma-\frac{4}{3}\right))^2$

$=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$

$=D'$

$=-4\cdot\left(-\frac{196}{3}\right)^3-27\cdot\left(-\frac{560}{27}\right)^2=\ 2^{11}\cdot 7^2\cdot 11$

$\therefore\quad \sqrt{D'}=2^5\cdot 7\cdot\sqrt{22}\notin Q$

$\therefore\quad G\ \cong S_4$

<求め方 2 >　フェラーリの解法で解を求めると、

$x^4=-2x^2-8x-16$

$\therefore\quad x^4+2\lambda x^2+\lambda^2=-2x^2-8x-16+2\lambda x^2+\lambda^2$

$\therefore\quad (x^2+\lambda)^2=(2\lambda-2)x^2-8x+\lambda^2-16$

右辺が完全平方式になるには、判別式＝ 0 が必要で

$(-4)^2-(2\lambda-2)(\lambda^2-16)=0$

$\lambda^3-\lambda^2-16\lambda+8=0$

$\lambda=m+\frac{1}{3}$ とおくと、

$$m^3-\frac{49}{3}m+\frac{70}{27}=0$$

(これはガロア群 S_3 をもつ)

カルダノの公式より、解の 1 つは、

$$m=\sqrt[3]{-\frac{35}{27}+\sqrt{\left(\frac{35}{27}\right)^2+\left(-\frac{49}{9}\right)^3}}+\sqrt[3]{-\frac{35}{27}-\sqrt{\left(\frac{35}{27}\right)^2+\left(-\frac{49}{9}\right)^3}}$$

$$=\sqrt[3]{-\frac{35}{27}+\frac{14}{9}\sqrt{-66}}+\sqrt[3]{-\frac{35}{27}-\frac{14}{9}\sqrt{-66}}$$

$$=\frac{1}{3}\left(\sqrt[3]{-35+42\sqrt{-66}}+\sqrt[3]{-35-42\sqrt{-66}}\right)$$

$$\therefore\ \lambda=\frac{1}{3}\left(1+\sqrt[3]{-35+42\sqrt{-66}}+\sqrt[3]{-35-42\sqrt{-66}}\right)$$

（注意：$\sqrt[3]{-35-42\sqrt{-66}}=\frac{49}{\sqrt[3]{-35+42\sqrt{-66}}}$ ，$\sqrt{-66}=\sqrt{22}\cdot\sqrt{-3}=\sqrt{22}(2\omega+1)$ ）

このとき、

$$(x^2+\lambda)^2=(2\lambda-2)\left(x-\frac{4}{2\lambda-2}\right)^2$$

$$\therefore\ x^2+\lambda=\pm\sqrt{2\lambda-2}\left(x-\frac{4}{2\lambda-2}\right)$$

$$\therefore\ x^2+\lambda=\sqrt{2\lambda-2}\,x-\frac{4}{\sqrt{2\lambda-2}}\ ,\ x^2+\lambda=-\sqrt{2\lambda-2}\,x+\frac{4}{\sqrt{2\lambda-2}}$$

$$\therefore\ x^2-\sqrt{2\lambda-2}\,x+\lambda+\frac{4}{\sqrt{2\lambda-2}}=0\ ,\ x^2+\sqrt{2\lambda-2}\,x+\lambda-\frac{4}{\sqrt{2\lambda-2}}=0$$

これらより、

$$\therefore\quad x_1=\frac{(\lambda-1)+\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}}{\sqrt{2\lambda-2}}$$

$$x_2=\frac{(\lambda-1)-\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}}{\sqrt{2\lambda-2}}$$

$$x_3=\frac{-(\lambda-1)+\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}}{\sqrt{2\lambda-2}}$$

$$x_4=\frac{-(\lambda-1)-\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}}{\sqrt{2\lambda-2}}$$

（注意:　$\lambda^3-\lambda^2-16\lambda+8=0$ より

$$\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}} = \frac{\sqrt{\lambda^4-2\lambda^2-32\lambda+33}}{\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}} = \frac{\sqrt{15\lambda^2-24\lambda+25}}{\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}} \quad)$$

これより、$\lambda = \frac{1}{3}\left(1+\sqrt[3]{-35+42\sqrt{-66}}+\sqrt[3]{-35-42\sqrt{-66}}\right)$ として

$Q(x_1,x_2,x_3,x_4) = Q(\sqrt{-66}, \sqrt[3]{-35+42\sqrt{-66}}, \sqrt{2\lambda-2}, \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}, \sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}})$

$= Q(\sqrt{-66}, \sqrt[3]{-35+42\sqrt{-66}}, \sqrt{2\lambda-2}, \sqrt{15\lambda^2-24\lambda+25}, \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}})$

からそれ自身への自己同型写像 σ は、以下の

A 群 $\{a_1, a_2, a_3, a_4, a_5, a_6\}$ と B 群 $\{b_1, b_2, b_3, b_4\}$ の組み合わせより、

$6\times 4 = 24$ 通り考えられ、ガロア群 $G \cong S_4$（？）

A 群

$a_1 : \sqrt{-66} \to \sqrt{-66}, \sqrt[3]{-35+42\sqrt{-66}} \to \sqrt[3]{-35+42\sqrt{-66}}$

（このとき $\sqrt[3]{-35-42\sqrt{-66}} \to \sqrt[3]{-35-42\sqrt{-66}}$ ）

$a_2 : \sqrt{-66} \to \sqrt{-66}, \sqrt[3]{-35+42\sqrt{-66}} \to \sqrt[3]{-35+42\sqrt{-66}}\cdot\omega$

（このとき $\sqrt[3]{-35-42\sqrt{-66}} \to \sqrt[3]{-35-42\sqrt{-66}}\cdot\omega^2$）

$a_3 : \sqrt{-66} \to \sqrt{-66}, \sqrt[3]{-35+42\sqrt{-66}} \to \sqrt[3]{-35+42\sqrt{-66}}\cdot\omega^2$

（このとき $\sqrt[3]{-35-42\sqrt{-66}} \to \sqrt[3]{-35-42\sqrt{-66}}\cdot\omega$）

$a_4 : \sqrt{-66} \to -\sqrt{-66}, \sqrt[3]{-35+42\sqrt{-66}} \to \sqrt[3]{-35-42\sqrt{-66}}$

（このとき $\sqrt[3]{-35-42\sqrt{-66}} \to \sqrt[3]{-35+42\sqrt{-66}}$ ）

$a_5 : \sqrt{-66} \to -\sqrt{-66}, \sqrt[3]{-35+42\sqrt{-66}} \to \sqrt[3]{-35-42\sqrt{-66}}\cdot\omega$

（このとき $\sqrt[3]{-35-42\sqrt{-66}} \to \sqrt[3]{-35+42\sqrt{-66}}\cdot\omega^2$ ）

$a_6 : \sqrt{-66} \to -\sqrt{-66}, \sqrt[3]{-35+42\sqrt{-66}} \to \sqrt[3]{-35-42\sqrt{-66}}\cdot\omega^2$

（このとき $\sqrt[3]{-35-42\sqrt{-66}} \to \sqrt[3]{-35+42\sqrt{-66}}\cdot\omega$ ）

B 群 （ $\lambda = \frac{1}{3}\left(1+\sqrt[3]{-35+42\sqrt{-66}}+\sqrt[3]{-35-42\sqrt{-66}}\right)$ として）

$b_1 : \sqrt{15\lambda^2-24\lambda+25} \to \sqrt{15\lambda^2-24\lambda+25}$

$, \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}} \to \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}$

（このとき, $\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}} \to \sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}$ ）

$b_2 : \sqrt{15\lambda^2-24\lambda+25} \to -\sqrt{15\lambda^2-24\lambda+25}$

$, \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}} \to \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}$

（このとき, $\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}} \to -\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}$ ）

$b_3 : \sqrt{15\lambda^2-24\lambda+25} \to \sqrt{15\lambda^2-24\lambda+25}$

$, \sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}} \to -\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}$

（このとき, $\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}} \to -\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}$ ）

b_4 ： $\sqrt{15\lambda^2-24\lambda+25} \to -\sqrt{15\lambda^2-24\lambda+25}$

, $\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}} \to -\sqrt{-\lambda^2+1-4\sqrt{2\lambda-2}}$

（このとき, $\sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}} \to \sqrt{-\lambda^2+1+4\sqrt{2\lambda-2}}$ ）

例 5　$x^4+x^3+x^2+x+1=0$ (Q 上既約)のガロア群G

<求め方 1>

$x=y-\frac{1}{4}$で変換すると

$f(y)=y^4+\frac{5}{8}y^2+\frac{5}{8}y+\frac{205}{256}$

分解多項式は、

$g(y)=\frac{1}{64}(64y^3-80y^2-180y+25)$

$=\frac{1}{64}(4y+5)(16y^2-40y+5)$

∴ $g(x)=\frac{1}{64}(4x+6)(16x^2-32x-4)$

$=\frac{1}{8}(2x+3)(4x^2-8x-1)$

$g(x)$ がQ 上で 1 次と 2 次の因数に分解される。

一方、 $g(x)$ の最小分解体は、$M=Q(\sqrt{5})$ であって

$x^4+x^3+x^2+x+1$ は、$M=Q(\sqrt{5})$ 上可約である。

実際に

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

よって、ガロア群$G \cong C_4$

<求め方 2>

$x^4+x^3+x^2+x+1=0$ の解は、

$x^5-1=0$ の解のうち、$x=1$ を除いたもので、

$x=\cos\theta+i\sin\theta \quad (0\le\theta<2\pi)$ とおくと

$x^5=\cos(5\theta)+i\sin(5\theta)=1$　より

$5\theta=2\pi\ ,4\pi\ ,6\pi\ ,8\pi$ であり($5\theta=0$ を除く)

$\theta=2\pi/5\ ,4\pi/5\ ,6\pi/5\ ,8\pi/5$

∴ $x_1=\cos(2\pi/5)+i\sin(2\pi/5)=\xi$

$x_2=\cos(4\pi/5)+i\sin(4\pi/5)=\xi^2$

$x_3=\cos(6\pi/5)+i\sin(6\pi/5)=\xi^3$

$x_4 = \cos(8\pi/5) + i\sin(8\pi/5) = \xi^4$

$Q(\xi)$ からそれ自身への自己同型写像 σ は,

$\xi^5 = 1$ に注意して、

$\sigma_0 = i : \xi \to \xi$ $\quad (\xi^2 \to \xi^2,\ \xi^3 \to \xi^3,\ \xi^4 \to \xi^4)$

$\sigma_1 = \sigma : \xi \to \xi^2$ $\quad (\xi^2 \to \xi^4,\ \xi^3 \to \xi,\ \xi^4 \to \xi^3)$

$\sigma_2 = \sigma^2 : \xi \to \xi^4$ $\quad (\xi^2 \to \xi^3,\ \xi^3 \to \xi^2,\ \xi^4 \to \xi)$

$\sigma_3 = \sigma^3 : \xi \to \xi^3$ $\quad (\xi^2 \to \xi,\ \xi^3 \to \xi^4,\ \xi^4 \to \xi^2)$

である。

$x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4$ で書くと

$$i = \begin{pmatrix}1234\\1234\end{pmatrix},\ \sigma = \begin{pmatrix}1234\\2413\end{pmatrix},\ \sigma^2 = \begin{pmatrix}1234\\4321\end{pmatrix},\ \sigma^3 = \begin{pmatrix}1234\\3142\end{pmatrix}$$

これより

$G \cong \{ i, \sigma, \sigma^2, \sigma^3 \} \cong C_4$

ここから

Q 上可約な場合

例 6　$x^4 - 5x^2 + 6 = 0$（Q 上可約)のガロア群G

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

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

これは、$L = Q(\sqrt{2}, \sqrt{3})$ 上で

$f(x) = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$ と

異なる 1 次因数の積に分解されるから

L が$f(x)$ の最小分解体で

$i : \sqrt{2} \to \sqrt{2}$ $\quad, \sqrt{3} \to \sqrt{3}$

$\sigma : \sqrt{2} \to \sqrt{2}$ $\quad, \sqrt{3} \to -\sqrt{3}$

$\tau : \sqrt{2} \to -\sqrt{2}$ $\quad, \sqrt{3} \to \sqrt{3}$

$\sigma\tau : \sqrt{2} \to -\sqrt{2}$ $\quad, \sqrt{3} \to -\sqrt{3}$

とすれば、 $x_1 = -\sqrt{2} = \alpha, x_2 = \sqrt{2} = \beta,$

$x_3 = -\sqrt{3} = \gamma, x_4 = \sqrt{3} = \delta$ で表したとき

$$i = \begin{pmatrix}\alpha\beta\gamma\delta\\\alpha\beta\gamma\delta\end{pmatrix},\ \sigma = \begin{pmatrix}\alpha\beta\gamma\delta\\\alpha\beta\delta\gamma\end{pmatrix},\ \tau = \begin{pmatrix}\alpha\beta\gamma\delta\\\beta\alpha\gamma\delta\end{pmatrix},\ \tau\sigma = \begin{pmatrix}\alpha\beta\gamma\delta\\\beta\alpha\delta\gamma\end{pmatrix}$$ となり、

$G = G(L/Q) = \{i, \sigma, \tau, \sigma\tau\}$

これは、置換群 $\{i, (12), (34), (12)(34)\}$ に同型で

さらに、これは、

$\mathrm{V}=\{(\,),(12)(34),(13)(24),(14)(23)\}$に同型。（下注）

（注意）

W=$\{i\ ,(12)\ ,(34)\ ,(12)(34)\}$ で　$(1\ 2)=a$,$(3\ 4)=b$ とし、

$\mathrm{V}=\{(\,),(12)(34),(13)(24),(14)(23)\}$ で $(1\ 2)(3\ 4)=c$,

$(1\ 3)(2\ 4)=d$ とすれば、$(1\ 4)(2\ 3)=cd$ となり、

同じ群表が得られ、W≅Ｖ といえる。

W

	i	a	b	ab
i	i	a	b	ab
a	a	i	ab	b
b	b	ab	i	a
ab	ab	b	a	i

V

	()	c	d	cd
()	()	c	d	cd
c	c	()	cd	d
d	d	cd	()	c
cd	cd	d	c	()

例 7　$x^4-x^3+x^2-1=0$（Q 上可約)のガロア群G

$f(x)=x^4-x^3+x^2-1$

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

$x=1$ は、Q の元であり自己同型写像で不変なので

$f(x)$ のガロア群は、$f_1(x)=x^3+x+1$ のガロア群に同型で、

$D=-4\cdot1^3-27\cdot1^2=-31<0$ より

$\therefore\ \sqrt{D}\notin Q$

$\therefore\ G\cong S_3$

例 8　$x^4+x^2+1=0$（Q 上可約)のガロア群G

$f(x)=x^4+x^2+1$

$=x^4+2x^2+1-x^2$

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

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

これは、$L = Q(\sqrt{-3}\,)$ 上で

$f(x) = \left(x - \frac{1+\sqrt{-3}}{2}\right)\left(x - \frac{1-\sqrt{-3}}{2}\right)\left(x - \frac{-1+\sqrt{-3}}{2}\right)\left(x - \frac{-1-\sqrt{-3}}{2}\right)$ と

異なる 1 次因数の積に分解されるから、L が$f(x)$ の最小分解体で

$i:\ \sqrt{-3} \to \sqrt{-3}$

$\sigma:\ \sqrt{-3} \to -\sqrt{-3}$　　とすれば、

$x_1 = \dfrac{1+\sqrt{-3}}{2} = \alpha\ , x_2 = \dfrac{1-\sqrt{-3}}{2} = \beta\ ,$

$x_3 = \frac{-1+\sqrt{-3}}{2} = \gamma\ , x_4 = \frac{-1-\sqrt{-3}}{2} = \delta$ で表したとき

$i = \begin{pmatrix} \alpha\beta\gamma\delta \\ \alpha\beta\gamma\delta \end{pmatrix}$,$\sigma = \begin{pmatrix} \alpha\beta\gamma\delta \\ \beta\alpha\delta\gamma \end{pmatrix}$ となり、

$G = G(L/Q) = \{i\,, \sigma\,\}$

これは、置換群 $\{i\ , (12)(34)\}$ に同型で、S_2 に同型である。

【引用、参考文献】

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」
結城　浩著「数学ガール ガロア理論」
山下純一著「ガロアへのレクイエム」
矢ケ部　巌著「数Ⅲ方式ガロア理論」
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」