低次のGalois拡大の具体例を作るときに知っていると便利な判別式の話

黒木玄

判別式 $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ の根の差積を $\Delta(\overset{\alpha=(\alpha_1,\dots,\alpha_n)}{\overset{\downarrow}{\alpha}}) = \prod_{1\leqq i<j\leqq n}(\alpha_i-\alpha_j)$

と書く。これの2乗 $\Delta(\alpha)^2$ を多項式 $f(x)$ の<u>判別式</u> (discreminant) と呼ぶ。

判別式 $\Delta(\alpha)^2$ は次のような $2n-1$ 次の行列式で表わされる：

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n, \quad f'(x) = nx^n + (n-1)a_1x^{n-2} + \cdots + a_{n-1}$$

のとき，

$$\Delta(\alpha)^2 = (-1)^{n(n-1)/2}\begin{array}{c} \overbrace{\hphantom{1\quad a_1\quad\cdots\quad a_n}}^{n+1}\ \overbrace{\hphantom{\quad\cdots\quad a_n}}^{n-2} \\ \begin{vmatrix} 1 & a_1 & \cdots & a_n & & \\ & \ddots & \ddots & & \ddots & \\ & & 1 & a_1 & \cdots & a_n \\ n & (n-1)a_1 & \cdots & a_{n-1} & & \\ & \ddots & \ddots & & \ddots & \\ & & n & (n-1)a_1 & \cdots & a_{n-1} \end{vmatrix} \\ \underbrace{\hphantom{n\quad\ddots}}_{n-1}\ \underbrace{\hphantom{n\quad (n-1)a_1\quad\cdots\quad a_{n-1}}}_{n} \end{array} \begin{array}{l} \left.\vphantom{\begin{matrix}1\\ \ddots\\ 1\end{matrix}}\right\} n-1 \\ \left.\vphantom{\begin{matrix}1\\ \ddots\\ 1\end{matrix}}\right\} n \end{array}. \quad \square$$

もしくは佐武一郎『線型代数学』第II章§6の1を参照せよ。

証明を知りたければ Sylvester resultant について検索せよ。

例 $f(x) = x^2 + px + q = (x-\alpha)(x-\beta)$ のとき,

$$(-1)^{2\cdot 1/2}\begin{vmatrix} 1 & p & q \\ 2 & p & \\ & 2 & p \end{vmatrix} = -(p^2 + 4q - 2p^2) = p^2 - 4q.$$

$$(\alpha-\beta)^2 = (\alpha+\beta)^2 - 4\alpha\beta = (-p)^2 - 4q = p^2 - 4q. \qquad \square$$

例 $f(x) = x^3 + px + q = (x-\alpha)(x-\beta)(x-\gamma)$ のとき,

$$(-1)^{3\cdot 2/2}\begin{vmatrix} 1 & 0 & p & q & \\ & 1 & 0 & p & q \\ 3 & 0 & p & & \\ & 3 & 0 & p & \\ & & 3 & 0 & p \end{vmatrix} = -\left|\begin{array}{cc|ccc} 1 & 0 & p & q & \\ & 1 & 0 & p & q \\ \hline 0 & 0 & -2p & -3q & \\ & 0 & 0 & -2p & -3q \\ & & 3 & 0 & p \end{array}\right| = -(4p^3 + 27q^2) = -4p^3 - 27q^2.$$

$$\left(\begin{array}{l} \alpha+\beta+\gamma = 0, \quad \alpha\beta+\alpha\gamma+\beta\gamma = p, \quad \alpha\beta\gamma = -q \\ 0 = (\alpha+\beta+\gamma)^2 = \alpha^2+\beta^2+\gamma^2+2p \quad \therefore \ \alpha^2+\beta^2+\gamma^2 = -2p \\ p^2 = (\alpha\beta+\alpha\gamma+\beta\gamma)^2 = \alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2 \end{array}\right)$$

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

$$= -\left(p^3 + 3(-2p)p^2 + 9p^2p + 27(-q)^2\right) = -(4p^3+27q^2) = -4p^3 - 27q^2. \qquad \square$$

$\boxed{\text{例}}$ $f(x) = x^4 + px + q = \prod_{i=1}^{4}(x-\alpha_i)$ のとき,

1つ前の例と同様

$$\Delta(\alpha)^2 = (-1)^{4\cdot 3/2} \begin{vmatrix} 1 & 0 & 0 & p & q & & \\ & 1 & 0 & 0 & p & q & \\ & & 1 & 0 & 0 & p & q \\ 4 & 0 & 0 & p & & & \\ & 4 & 0 & 0 & p & & \\ & & 4 & 0 & 0 & p & \\ & & & 4 & 0 & 0 & p \end{vmatrix} = -27p^4 + 256q^3. \qquad \square$$

$\boxed{\text{例}}$ $f(x) = x^4 + px^2 + q = \prod_{i=1}^{4}(x-\alpha_i)$ のとき,

$$\Delta(\alpha)^2 = (-1)^{4\cdot 3/2} \begin{vmatrix} 1 & 0 & p & 0 & q & & \\ & 1 & 0 & p & 0 & q & \\ & & 1 & 0 & p & 0 & q \\ 4 & 0 & 2p & 0 & & & \\ & 4 & 0 & 2p & 0 & & \\ & & 4 & 0 & 2p & 0 & \\ & & & 4 & 0 & 2p & 0 \end{vmatrix} = 16q(p^2-4q)^2. \qquad \square$$

これらの公式の応用例については以下の文献を参照せよ.

https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf
https://people.math.carleton.ca/~williams/papers/pdf/232.pdf

佐武一郎著『線型代数学』§6の1の最後の問1の解答例

(x^n+ax+b の判別式)

$$
= (-1)^{n(n-1)/2}
\begin{array}{c}
\overbrace{\qquad\qquad\quad}^{n+1}\overbrace{\qquad}^{n-2} \\
\begin{vmatrix}
1 & 0 & \cdots & 0 & a & b & & & \\
 & 1 & 0 & \cdots & 0 & a & b & & \\
 & & \ddots & & & \ddots & & \ddots & \\
 & & & 1 & 0 & \cdots & 0 & a & b \\
n & 0 & \cdots & 0 & a & & & & \\
 & n & 0 & \cdots & 0 & a & & & \\
 & & \ddots & & & \ddots & \ddots & & \\
 & & & & n & 0 & \cdots & 0 & a \\
 & & & & & n & 0 \cdots & 0 & a
\end{vmatrix}
\end{array}
\begin{array}{l}
\left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\} n-1 \\
\left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\end{matrix}}\right\} n
\end{array}
$$

第1,…,n-1行目の n 倍を第n,…,2n-2行目からひく

$$
= (-1)^{n(n-1)/2}
\left|\begin{array}{cccc|cccccc}
1 & 0 & \cdots & 0 & a & b & & & & \\
 & 1 & 0 & \cdots & 0 & a & b & & & \\
 & & \ddots & & & \ddots & \ddots & \ddots & & \\
 & & & 1 & \cdots & 0 & & a & b & \\
\hline
0 & 0 & \cdots & 0 & -(n-1)a & -nb & & & & \\
 & 0 & 0 & \cdots & 0 & -(n-1)a & -nb & & & \\
 & & \ddots & \ddots & & \ddots & \ddots & \ddots & & \\
 & & & 0 & 0 & \cdots & 0 & -(n-1)a & -nb & \\
 & & & & n & 0 & \cdots & 0 & a &
\end{array}\right|
\left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\end{matrix}}\right\} n
$$

一般に

$$
\begin{vmatrix} A & * \\ 0 & B \end{vmatrix} = |A|\,|B|
$$

$$
= (-1)^{n(n-1)/2}
\begin{vmatrix}
-(n-1)a & -nb & & & 0 \\
0 & -(n-1)a & -nb & & \\
\vdots & 0 & \ddots & \ddots & \\
\vdots & \vdots & \ddots & -(n-1)a & -nb \\
n & 0 & \cdots & 0 & a
\end{vmatrix}
\left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\end{matrix}}\right\} n
$$

第1列を右端に移動

$$
= (-1)^{n(n-1)/2}\left(
\begin{vmatrix}
-(n-1)a & -nb & & & 0 \\
0 & -(n-1)a & -nb & & \\
\vdots & 0 & \ddots & \ddots & \\
\vdots & \vdots & \ddots & -(n-1)a & -nb \\
0 & 0 & \cdots & 0 & a
\end{vmatrix}
+
\left|\begin{array}{c|cccc}
0 & -nb & & & 0 \\
0 & -(n-1)a & -nb & & \\
\vdots & 0 & \ddots & \ddots & \\
\vdots & \vdots & \ddots & -(n-1)a & -nb \\
\hline
n & 0 & \cdots & 0 & a
\end{array}\right|
\right)
$$

$$
= (-1)^{n(n-1)/2}\left(
\begin{vmatrix}
-(n-1)a & -nb & & & 0 \\
0 & -(n-1)a & -nb & & \\
\vdots & 0 & \ddots & \ddots & \\
\vdots & \vdots & \ddots & -(n-1)a & -nb \\
0 & 0 & \cdots & 0 & a
\end{vmatrix}
+ (-1)^{n-1}
\left|\begin{array}{cccc|c}
-nb & & & 0 & 0 \\
-(n-1)a & -nb & & & 0 \\
0 & \ddots & \ddots & & \vdots \\
\vdots & \ddots & -(n-1)a & -nb & \vdots \\
\hline
0 & \cdots & 0 & a & n
\end{array}\right|
\right)
$$

$$
= (-1)^{n(n-1)/2}\left((-1)^{n-1}(n-1)^{n-1}a^n + (-1)^{n-1}(-1)^{n-1}n^n b^{n-1}\right)
$$

$$
= (-1)^{n(n-1)/2}\left((-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}\right)
$$

$n=5$ の場合

(x^5+ax+b の判別式)

$$
= (-1)^{4\cdot 5/2}
\begin{vmatrix}
1 & 0 & 0 & 0 & a & b & & & \\
 & 1 & 0 & 0 & 0 & a & b & & \\
 & & 1 & 0 & 0 & 0 & a & b & \\
 & & & 1 & 0 & 0 & 0 & a & b \\
5 & 0 & 0 & 0 & a & & & & \\
 & 5 & 0 & 0 & 0 & a & & & \\
 & & 5 & 0 & 0 & 0 & a & & \\
 & & & 5 & 0 & 0 & 0 & a & \\
 & & & & 5 & 0 & 0 & 0 & a
\end{vmatrix}
$$

1,2,3,4行の5倍を5,6,7,8行から引く

$$
=
\left|\begin{array}{cccc|ccccc}
1 & 0 & 0 & 0 & a & b & & & \\
 & 1 & 0 & 0 & 0 & a & b & & \\
 & & 1 & 0 & 0 & 0 & a & b & \\
 & & & 1 & 0 & 0 & 0 & a & b \\
\hline
0 & 0 & 0 & 0 & -4a & -5b & & & \\
 & 0 & 0 & 0 & 0 & -4a & -5b & & \\
 & & 0 & 0 & 0 & 0 & -4a & -5b & \\
 & & & 0 & 0 & 0 & 0 & -4a & -5b \\
 & & & & 5 & 0 & 0 & 0 & a
\end{array}\right|
$$

$$
=
\begin{vmatrix}
-4a & -5b & & & \\
0 & -4a & -5b & & \\
0 & 0 & -4a & -5b & \\
0 & 0 & 0 & -4a & -5b \\
5 & 0 & 0 & 0 & a
\end{vmatrix}
$$

第1列についての行列式の線形性

$$
=
\begin{vmatrix}
-4a & -5b & & & \\
0 & -4a & -5b & & \\
0 & 0 & -4a & -5b & \\
0 & 0 & 0 & -4a & -5b \\
0 & 0 & 0 & 0 & a
\end{vmatrix}
+
\left|\begin{array}{c|cccc}
0 & -5b & & & \\
0 & -4a & -5b & & \\
0 & 0 & -4a & -5b & \\
0 & 0 & 0 & -4a & -5b \\
\hline
5 & 0 & 0 & 0 & a
\end{array}\right|
$$

$$
= (-4a)^4 a + 5(-5b)^4
$$

$$
= 4^4 a^5 + 5^5 b^4.
$$

定理 体K上既約な分離的n次多項式 $f(x) \in K[x]$ の最小分解体をLと書き, $f(x)$ の根の全体の集合を $A = \{\alpha_1, \dots, \alpha_n\}$ と書き, Aの置換と置換群 S_n を同一視しておく. このとき, $\mathrm{Gal}(L/K)$ は A に置換として作用し, それによって, S_n に単射的に埋め込まれる. その像を $\mathrm{Gal}(f) = \mathrm{Gal}(f/K)$ と書くことにする. このとき, $\mathrm{Gal}(f) = \mathrm{Gal}(f/K)$ は S_n の推移的部分群になる. (この結果は演習で説明した.) このとき,

$$\Delta(\alpha) = \prod_{1 \leqq i < j \leqq n} (\alpha_i - \alpha_j) \in K \iff \mathrm{Gal}(f) < A_n.$$

差積

証明 $\Leftarrow$ を示そう. $\mathrm{Gal}(f) < A_n$ ならば任意の $\sigma \in \mathrm{Gal}(f)$ について $\sigma(\Delta(\alpha)) = \Delta(\alpha)$ となるので $\Delta(\alpha) \in K$ となる.

偶置換になる

偶置換 $\iff$ その作用で差積が不変

$\Rightarrow$ の対偶を示そう. $\mathrm{Gal}(f) < A_n$ でないならば奇置換 $\sigma \in \mathrm{Gal}(f)$ が存在し, $\sigma(\Delta(\alpha)) = -\Delta(\alpha) \neq \Delta(\alpha)$ となるので $\Delta(\alpha) \notin K$ となる. $\square$

注 $\forall \beta \in L$ について, $\beta \in K \iff \forall \sigma \in \mathrm{Gal}(L/K),\ \sigma(\beta) = \beta$.

S_nの推移的部分群の例

S_3の部分群は $S_3, A_3, \langle(1,2)\rangle, \langle(1,3)\rangle, \langle(2,3)\rangle, \{1\}$ の5つしかない。

S_3の推移的部分群の全体 S_3, A_3 の2つだけ。 $\square$

ゆえに既約な3次分離多項式 $f(x) \in K[x]$ について, $\mathrm{Gal}(f/K) \cong S_3, A_3$, この2つの可能性しかない。そして,

$$\text{判別式 } \Delta(\alpha)^2 \text{ の平方根が } K \text{ に含まれる} \iff \mathrm{Gal}(f/K) \cong A_3$$

$\Delta(\alpha)^2$は常にKに含まれる。($\because$ $\forall \sigma \in \mathrm{Gal}(L/K)$, $\sigma(\Delta(\alpha)^2) = (\pm\Delta(\alpha))^2 = \Delta(\alpha)^2$)

例 $f(x) = x^3 - 2$ の判別式は $-4 \cdot 0^3 - 27(-2)^2 = -3 \cdot 6^2$.

$\sqrt{-3 \cdot 6^2} = 6\sqrt{-3} \notin \mathbb{Q}$ より, $\mathrm{Gal}(f/\mathbb{Q}) \cong S_3$.

注 $f(x)$は$\mathbb{Q}(\omega)$上既約.

ωを1の原始3乗根とすると, $\omega = \dfrac{-1+\sqrt{-3}}{2}$ なので, $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ となり,

$\sqrt{-3 \cdot 6^2} = 6\sqrt{-3} \in \mathbb{Q}(\omega)$ となる。ゆえに, $\mathrm{Gal}(f/\mathbb{Q}(\omega)) \cong A_3$.

$\square$

例 $f(x) = x^3 - 3x - 1$ の判別式は $-4(-3)^3 - 27(-1)^2 = 9^2$ で $\sqrt{9^2} = 9 \in \mathbb{Q}$.

ゆえに, $\mathrm{Gal}(f/\mathbb{Q}) \cong A_3$.

$\square$

一般に S_n の推移的部分群 G に対して，$X_i=\{\sigma\in G \mid \sigma(1)=i\}$ とおくと，
$G=X_1\sqcup\cdots\sqcup X_n$ かつ $\sigma\in X_i$ について $\sigma X_1=X_i$ より，$|X_1|=\cdots=|X_n|$ が成立するので，
G の位数は n の倍数になる。

$\boxed{S_4\text{ の部分群の例}}$ （ある $\sigma\in S_4$ による $H \xmapsto{\text{共役}} \sigma H\sigma^{-1}$ のちがいを除いて以下しかない。）

位数	部分群	
1	$\{1\}$	
2	$\langle(1,2)\rangle$, $\langle(1,2)(3,4)\rangle$	
3	$\langle(1,2,3)\rangle$	
4	$\langle(1,2,3,4)\rangle\cong C_4$, $V_4=\{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$, $\langle(1,2),(3,4)\rangle\cong C_2\times C_2$	巡回群 (C_4)；Kleinの四元群 (V_4)
6	$\langle(1,2,3),(1,2)\rangle$	
8	$\langle(1,2,3,4),(2,4)\rangle\cong D_4$	二面体群
12	A_4	← 交代群
24	S_4	

この中で推移的なのは

$$\begin{cases}\langle(1,2,3,4)\rangle = C_4,\ V_4,\\ \langle(1,2,3,4),(2,4)\rangle\cong D_4,\ A_4,\ S_5\end{cases}$$

の5種類

$\boxed{例}$ $f(x) = x^4 - 2$. 判別式は $256(-2)^3 = -2\cdot 32^2$.　　注 x^4-2 は $\mathbb{Q}(\sqrt{-1})$ 上既約

$\sqrt{-2\cdot 32^2} \notin \mathbb{Q}$ より, $\mathrm{Gal}(f/\mathbb{Q}) \not\subset A_4$. 実際, $\mathrm{Gal}(f/\mathbb{Q}) \cong D_4 \not\subset A_4$.

$\sqrt{-2\cdot 32^2} \notin \mathbb{Q}(\sqrt{-1})$ より, $\mathrm{Gal}(f/\mathbb{Q}(\sqrt{-1})) \not\subset A_4$. 実際, $\mathrm{Gal}(f/\mathbb{Q}(\sqrt{-1})) \cong C_4 \not\subset A_4$

$(1,2,3,4) = (1,2)(2,3)(3,4)$ は奇置換なので $(1,2,3,4) \notin A_4$.

x^4-2 の最小分解体は $L = \mathbb{Q}(\sqrt{-1}, \sqrt[4]{2})$ であることより,

$$\mathrm{Gal}(L/\mathbb{Q}) \cong D_4, \quad \mathrm{Gal}(L/\mathbb{Q}(\sqrt{-1})) \cong C_4.$$

□

$\boxed{例}$ $f(x) = x^4 - 10x^2 + 1 = (x-(\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$.

判別式は $16\cdot 1((-10)^2-4\cdot 1)^2 = (4\cdot 96)^2$ でこれの平方根 $\in \mathbb{Q}$ となる.

ゆえに, $\mathrm{Gal}(f/\mathbb{Q}) \subset A_4$. 実際, $\mathrm{Gal}(f/\mathbb{Q}) \cong V_4 \subset A_4$.　　注 x^4-10x^2+1 は $\mathbb{Q}$ 上既約

x^4-10x^2+1 の最小分解体は $L = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ で

$$\mathrm{Gal}(L/\mathbb{Q}) \cong C_2 \times C_2 \cong V_4.$$

□

$\{\sqrt{2}+\sqrt{3}, -\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3}\}$ への作用を見る.

$\boxed{\text{例}}$ $f(x) = x^4 + 36x + 63 = (x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$, ← $\mathbb{Q}$上既約になる

$$\alpha = \frac{-3+(\sqrt{2}-1)\sqrt{-3}}{\sqrt{2}},\quad \beta = \frac{-3-(\sqrt{2}-1)\sqrt{-3}}{\sqrt{2}},\quad \gamma = \frac{3+(\sqrt{2}+1)\sqrt{-3}}{\sqrt{2}},\quad \delta = \frac{3-(\sqrt{2}+1)\sqrt{-3}}{\sqrt{2}}.$$

$f(x)$の最小分解体は $L = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ で, $\mathrm{Gal}(L/\mathbb{Q}) \cong C_2 \times C_2 \cong V_4$.

$\{\alpha, \beta, \gamma, \delta\}$への作用を見る　Kleinの四元群

$$(f(x)\text{の判別式}) = -27\cdot \underbrace{36^4}_{3^3\cdot 2^8\cdot 3^8} + 256\cdot 63^3 = -2^8\cdot 3^{11} + 2^8\cdot 3^6\cdot 7^3$$
$$= 2^8\cdot 3^6(7^3 - 3^5) = 2^8\cdot 3^6\cdot 100 = 2^{10}\cdot 3^6\cdot 5^2$$

ゆえに(判別式の平方根) $\in \mathbb{Q}$ となるので, $\mathrm{Gal}(f/\mathbb{Q}) \subset A_4$.

実際 $\mathrm{Gal}(f/\mathbb{Q}) = V_4 \subset A_4$.

$\square$

この例は次の文献の p.8 の Table 5 にある:

https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf

$\boxed{\text{定理}}$ (渡辺敬一・草場公邦『代数の世界』pp. 231−235) 以下, 標数0とする.

体K上既約な4次の多項式 $f(x) = x^4 + ax^2 + bx + c \in K[x]$ を考える.

$g(\lambda) = \lambda^3 + 2a\lambda^2 + (a^2 - 4c)\lambda - b^2$ とおき, $g(\lambda)$ のK上での最小分解体をMと書く.

$f(x)$ の判別式を $D = \Delta(\alpha)^2$ と書く.

証明は略

(1) $g(\lambda)$ がK上既約なとき,

$$\begin{cases} \sqrt{D} = \Delta(\alpha) \in K \Rightarrow \mathrm{Gal}(f/K) = A_4, \\ \sqrt{D} = \Delta(\alpha) \notin K \Rightarrow \mathrm{Gal}(f/K) = S_4. \end{cases}$$

(2) $g(\lambda)$ が $K[x]$ 内で既約な2次式と1次式の積に分解するとき,

$$\begin{cases} f(x) \text{ が } M \text{ 上既約} \Rightarrow \mathrm{Gal}(f/K) \cong D_4, \\ f(x) \text{ が } M[x] \text{ 内で2つの既約2次式に分解} \Rightarrow \mathrm{Gal}(f/K) \cong C_4. \end{cases}$$

(3) $g(\lambda)$ が $K[x]$ 内で3つの1次式の積に分解するとき, $\mathrm{Gal}(f/K) = V_4$.

$\boxed{\text{注意}}$ $f(x)$ と $g(\lambda)$ の判別式は等しい. □

前ページの $f(x)$ と $g(x)$ の関係　　4次方程式の解法

仮に $f(x) = x^4 + ax^2 + bx + c$ が次のように書けたとする:

$$
\begin{aligned}
f(x) &= (x+p+q+r)(x+p-q-r)(x-p+q-r)(x-p-q+r) \\
&= x^4 - 2(p^2+q^2+r^2)x^2 + 8pqr\,x + p^4+q^4+r^4 - 2(p^2q^2+p^2r^2+q^2r^2) \\
&= x^4 \underbrace{-2(p^2+q^2+r^2)}_{=a}x^2 + \underbrace{8pqr}_{=b}\,x + \underbrace{(p^2+q^2+r^2)^2 - 4(p^2q^2+p^2r^2+q^2r^2)}_{=c}
\end{aligned}
$$

$A = 4(p^2+q^2+r^2)$, $B = 16(p^2q^2+p^2r^2+q^2r^2)$, $C = 64p^2q^2r^2$ とおくと,　A, B, C は $4p^2, 4q^2, 4r^2$ の基本対称式.

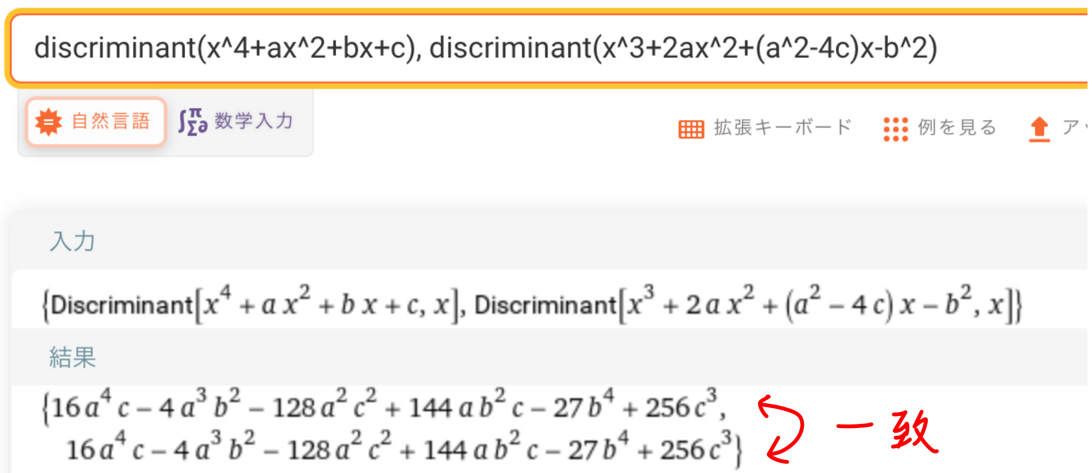
$a = -\frac{1}{2}A$,　$b^2 = C$,　$c = \frac{1}{16}A^2 - \frac{1}{4}B = \frac{1}{4}a^2 - \frac{1}{4}B$　すなわち　$A = -2a$,　$B = a^2 - 4c$,　$C = b^2$.

ゆえに, $f(x)$ が上のように書けることと, $4p^2, 4q^2, 4r^2$ が3次方程式

$$g(\lambda) = \lambda^3 - A\lambda^2 + B\lambda - C = \lambda^3 + 2a\lambda^2 + (a^2-4c)\lambda - b^2 = 0$$

の3つの解になることは同値である. そのとき, 4次方程式 $f(x)=0$ の4つの解は次のように書ける.

$$x = -p-q-r,\quad -p+q+r,\quad p-q-r,\quad p+q-r$$



一致

WolframAlpha による $f(x)$ と $g(x)$ の判別式の一致の確認

https://www.wolframalpha.com/input?i=discriminant%28x%5E4%2Bax%5E2%2Bbx%2Bc%29%2C+discriminant%28x%5E3%2B2ax%5E2%2B%28a%5E2-4c%29x-b%5E2%29&lang=ja

$\boxed{\text{例}}$ $f(x) = x^4 + 36x + 63$ のとき, $g(\lambda) = \lambda^3 - 4\cdot 63\lambda + 36^2 = (\lambda+6)(\lambda+12)(\lambda-18)$

なので, $\mathrm{Gal}(f/\mathbb{Q}) = V_4$ (Kleinの四元群). ← 前々ページの(3)の場合

$\square$

$\boxed{\text{例}}$ $f(x) = x^4 - 2$ のとき, $g(\lambda) = \lambda^3 + 8\lambda = \lambda(\lambda^2 + 8)$.

$g(\lambda)$ の $\mathbb{Q}$ 上での最小分解体は $M = \mathbb{Q}(\sqrt{-2})$.

$f(x)$ は M 上でも既約である. ゆえに, $\mathrm{Gal}(f/\mathbb{Q}) \cong D_4$.

前々ページの(2)上段の場合

$g(\lambda)$ の $\mathbb{Q}(\sqrt{-1})$ 上での最小分解体は $M' = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$.

前々ページの(2)下段の場合

$f(x)$ は $M'[x]$ の中で $f(x) = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$ と分解するので, $\mathrm{Gal}(f/\mathbb{Q}(\sqrt{-1})) \cong C_4$. $\square$

$\boxed{\text{例}}$ $f(x) = x^4 + 8x + 12$ は $\mathbb{Q}$ 上既約で, $g(\lambda) = \lambda^3 - 48\lambda - 64$ も $\mathbb{Q}$ 上既約である.

$(f\text{の判別式}) = -3^3\cdot 8^4 + 2^8\cdot 12^3 = -2^{12}\cdot 3^3 + 2^{14}\cdot 3^3 = 2^{12}\cdot 3^4$ なので $(\text{その平方根}) \in \mathbb{Q}$,

ゆえに $\mathrm{Gal}(f/\mathbb{Q}) = A_4$. 前々ページ(1)上段の場合

$\square$

$\boxed{\text{例}}$ $f(x) = x^4 + 2x + 2$ は $\mathbb{Q}$ 上既約で, $g(\lambda) = \lambda^3 - 8\lambda + 4$ も $\mathbb{Q}$ 上既約である.

$(f\text{の判別式}) = -3^3\cdot 2^4 + 2^8\cdot 2^3 = 1616 = 2^4\cdot 101$ なので $(\text{その平方根}) \notin \mathbb{Q}$.

ゆえに, $\mathrm{Gal}(f/\mathbb{Q}) = S_4$. 前々ページ(1)下段の場合

$\square$