

可解な代数方程式の ガロア理論に基づいた解法(第2版)

退職後は素人数学者 2019年 9月

目次

まえがき	2
<u>第1部 代数方程式のガロア群の計算法</u>	
1. 根 $x_1, x_2, \dots, x_n$ の関係式	4
2. $x_1, x_2, \dots, x_n$ からなる多項式の次数低減	6
3. $x_1, x_2, \dots, x_n$ の置換 $\sigma_1, \sigma_2, \dots, \sigma_n!$	8
4. 原始要素 v とその最小多項式 $g(x)$	9
5. $f(x)$ の分解体の基底 $w_1, w_2, \dots, w_{n!}$	17
6. $x_1, x_2, \dots, x_n$ の v による多項式表現	19
7. ガロア群 G の計算法	23
8. ガロア群 G の乗積表と逆元	26
9. ガロア群 G の組成列	29
10. 数式処理ソフトによる計算	34
<u>第2部 可解な代数方程式の解法</u>	
11. $f(x)$ の分解体に属する元の表記と積・商の計算	41
12. 体の拡大と $g(x)$ の次数低減	45
13. 根 $x_1, x_2, \dots, x_n$ の計算	52
14. 数式処理ソフトによる計算	54
<u>付録</u>	
15. 可解な5次方程式の解法	65
参考文献	71

まえがき

ガロア理論に関する本の大部分は、代数方程式が可解であるための条件を示したところで終わっていて、可解な代数方程式の解法まで述べたものはない。インターネットなどを探しても殆ど見つからないが、ようやく1件だけ探し当てることができた。それが参考文献(1)である。そこで述べられている方法を改めて整理し、数式処理ソフトMathematicaによる計算例を加えた。

本稿の第1版は、参考文献(1)の著者のご厚意により、同文献の2018年9月1日の記事に掲載されている。その後、参考文献(1)と参考文献(2)の間で議論が交わされ、いくつかの改良が提案されている。本稿の第2版は、いくつかの改良を取り入れて、書き直したものである。

第1部では代数方程式のガロア群の計算法について述べる。以下に概要を示す。

- (1) 対象とする代数方程式は n 次方程式 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ とし、その根を $x_1, x_2, \cdots, x_n$ とする。 $f(x)$ が $x-x_1, x-x_2, \cdots, x-x_n$ で割り切れることから、 $x_1, x_2, \cdots, x_n$ の間に成り立つ計 n 個の関係式を求める。
- (2) これを使うと、 $x_1, x_2, \cdots, x_n$ の多項式は $x_1^0x_2^0\cdots x_n^0$ から $x_1^{n-1}x_2^{n-2}\cdots x_n^0$ まで、計 $n!$ 個の項に集約される。
- (3) 根 $x_1, x_2, \cdots, x_n$ に関する $n!$ 通りの置換を $\sigma_1, \sigma_2, \cdots, \sigma_{n!}$ とする。
- (4) $v=m_1x_1+m_2x_2+\cdots+m_nx_n$ (m_i は相異なる整数) とし、 $\sigma_1, \sigma_2, \cdots, \sigma_{n!}$ で置換したものを $v_1, v_2, \cdots, v_{n!}$ とする。ここで、 $v_1, v_2, \cdots, v_{n!}$ が相異なる値となるように m_i を決めれば、 v は $f(x)$ の分解体の原始要素となる。 $(x-v_1)(x-v_2)\cdots(x-v_{n!})$ は x_i の対称式であるから、展開した後の各係数は $a_{n-1}, \cdots, a_1, a_0$ の多項式となる。これを有理係数の範囲で因数分解し、任意の1因数を $g(x)$ とすれば、これが v の最小多項式となる。
- (5) 上記(2)の $n!$ 個の項を $w_1, w_2, \cdots, w_{n!}$ と書くと、 $f(x)$ の分解体の元は $w_1, w_2, \cdots, w_{n!}$ の1次式で表せる。
- (6) $v^0, v^1, \cdots, v^{n!-1}$ は $w_1, w_2, \cdots, w_{n!}$ の1次式で表せる。逆に $w_1, w_2, \cdots, w_{n!}$ は $v^0, v^1, \cdots, v^{n!-1}$ の1次式で表せる。よって、根 $x_1, x_2, \cdots, x_n$ も $v^0, v^1, \cdots, v^{n!-1}$ の1次式、つまり v の $n!-1$ 次以下の多項式で表される。
- (7) $v_1, v_2, \cdots, v_{n!}$ の中で $g(x)$ の根であるものを v_i とする。これに対応する σ_i の集合がガロア群 G となる。
- (8) ガロア群 G の乗積表と逆元を求める。これは G の正規部分群を求めるのに使われる。
- (9) G の組成列 $G=G_0\supset G_1\supset\cdots\supset G_s$ を求める。 G_k ($k=1, 2, \cdots, s$) は G_{k-1} の正規部分群、 G_s は単位群である。
- (10) 以上の計算について、数式処理ソフトMathematicaによるプログラムと計算例を示した。

第2部では可解な代数方程式の解法について述べる。以下に概要を示す。

- (11) G の組成列に対応する体の拡大を $F_0 \subset F_1 \subset \cdots \subset F_s$ とする。 F_0 は $f(x)$ の係数体、 F_s は分解体である。 k 番の組成列 $G_{k-1} \supset G_k$ と拡大列 $F_{k-1} \subset F_k$ において、 $|G_{k-1}/G_k| = p_k$ (素数)、1の原始 p_k 乗根を ζ_{p_k} とする。 F_{k-1} の元と ζ_{p_k} との四則演算で作られる1つの数を A_k とし、 F_{k-1} に $\alpha_k = \sqrt[p_k]{A_k}$ を付加した体を F_k とする。以上より、 $f(x)$ の係数体 F_0 に $\alpha_1, \alpha_2, \dots, \alpha_s$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_s}$ を付加した体が $f(x)$ の分解体 F_s となる。
- (12) 体 F_0 上の最小多項式 $g(x)$ に続き、体 $F_1, F_2, \dots, F_s$ 上の最小多項式 $g_1(x), g_2(x), \dots, g_s(x)$ を求める。ここで、体 F_k 上の最小多項式は $g_k(x) = \prod (x - \sigma_i(v)) = \prod (x - v_i)$ (Π は $\sigma_i \in G_k$ に関する積を表す)で与える。詳細は本文で述べるが、上記のべき根 $\alpha_k = \sqrt[p_k]{A_k}$ を使うと、 $g_k(x)$ は α_k の p_k-1 次式に書き換えられる。 $\alpha_k^i (i=0, 1, \dots, p_k-1)$ に比例する項を $\theta_i(x)$ とすると、 $g_k(x) = \theta_0(x) + \theta_1(x) + \theta_2(x) + \cdots + \theta_{p_k-1}(x)$ と表される。
- (13) このようにして $g_1(x), g_2(x), \dots, g_s(x)$ を求めると、最後の $g_s(x)$ は1次式となり、 v が求められる。上記(6)より根 $x_1, x_2, \dots, x_n$ は v の多項式で表されるので、この v を代入すれば根 $x_1, x_2, \dots, x_n$ が求まる。
- (14) 以上の計算について、数式処理ソフトMathematicaによるプログラムと計算例を示した。

付録では以下を示す。

- (15) 可解な5次方程式の解法を示す。参考文献(3)を修正し、 x^3, x^2 の項があっても解けるようにした。

1. 根 $x_1, x_2, \dots, x_n$ の関係式

以下の n 次方程式について、根 $x_1, x_2, \dots, x_n$ の間に成り立つ関係式を求める。

$$f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0=0 \quad (1.1)$$

$f(x)$ を $x-x_1$ で割ったときの商を $q_1(x)$ 、余りを r_1 とすると、 r_1 は x_1 の n 次多項式となり、 $f(x)$ は $x-x_1$ で割り切れるから、 $r_1=0$ でなければならない。つぎに、 $q_1(x)$ を $x-x_2$ で割ったときの商を $q_2(x)$ 、余りを r_2 とすると、 r_2 は x_1, x_2 の $n-1$ 次多項式となり、 $q_1(x)$ は $x-x_2$ で割り切れるから、 $r_2=0$ でなければならない。同様に、最後は $q_{n-1}(x)$ を $x-x_n$ で割ったときの商を $q_n(x)$ 、余りを r_n とすると、 r_n は $x_1, x_2, \dots, x_n$ の1次多項式となり、 $q_{n-1}(x)$ は $x-x_n$ で割り切れるから、 $r_n=0$ でなければならない。以上をまとめると、余り $r_1, r_2, \dots, r_n$ は $x_1, x_2, \dots, x_n$ の多項式となり、これらには $r_1=0, r_2=0, \dots, r_n=0$ が成り立つ。これが、根 $x_1, x_2, \dots, x_n$ の間に成り立つ関係式となる。

(例) $f(x)=x^4+a_3x^3+a_2x^2+a_1x+a_0$ の場合

$f(x)$ を $x-x_1$ で割ると、 r_1 は x_1 の4次多項式となる。

$$q_1(x)=x^3+(x_1+a_3)x^2+(x_1^2+a_3x_1+a_2)x+x_1^3+a_3x_1^2+a_2x_1+a_1 \quad (1.2)$$

$$r_1=x_1^4+a_3x_1^3+a_2x_1^2+a_1x_1+a_0 \quad (1.3)$$

$q_1(x)$ を $x-x_2$ で割ると、 r_2 は x_1, x_2 の3次多項式となる。

$$q_2(x)=x^2+(x_1+x_2+a_3)x+x_1^2+x_1x_2+x_2^2+a_3(x_1+x_2)+a_2 \quad (1.4)$$

$$r_2=x_1^3+x_1^2x_2+x_1x_2^2+x_2^3+a_3(x_1^2+x_1x_2+x_2^2)+a_2(x_1+x_2)+a_1 \quad (1.5)$$

$q_2(x)$ を $x-x_3$ で割ると、 r_3 は x_1, x_2, x_3 の2次多項式となる。

$$q_3(x)=x+x_1+x_2+x_3+a_3 \quad (1.6)$$

$$r_3=x_1^2+x_1x_2+x_1x_3+x_2^2+x_2x_3+x_3^2+a_3(x_1+x_2+x_3)+a_2 \quad (1.7)$$

$q_3(x)$ を $x-x_4$ で割ると、 r_4 は x_1, x_2, x_3, x_4 の1次多項式となる。

$$q_4(x)=1 \quad (1.8)$$

$$r_4=x_1+x_2+x_3+x_4+a_3 \quad (1.9)$$

数式処理ソフトによる計算

《サブプログラム》

根 $X[1], X[2], \dots, X[n]$ の関係式 $r[1], r[2], \dots, r[n]$ を求める。

```
(* Relations of  $X[1], X[2], \dots, X[n]$  *)
RelationsOfX[fx_] := Module[{i, qx},
  qx = fx;
  For[i = 1, i <= n, i++,
    r[i] = PolynomialRemainder[qx, x - X[i], x];
    qx = PolynomialQuotient[qx, x - X[i], x]
  ]
];
```

ここで

```
RelationsOfX[fx_] := Module[{i, qx}, ...]
一般形はfunc[x_, y_, ...] := Module[{a, b, ...}, proc]である。
関数funcを定義する。x, y, ...は引数, a, b, ...はローカル変数, procは関数の手続き
procが複数の文からなる場合は各文を";"で区切る。
For[t1, t2, dt, proc] : 条件をt1からt2までdtずつ変えて, 手続きprocを反復する。
procが複数の文からなる場合は各文を";"で区切る。
PolynomialRemainder[f, g, x] : xの多項式f, gについて, fのgによる剰余を求める。
PolynomialQuotient[f, g, x] : xの多項式f, gについて, fのgによる商を求める。
```

《メインプログラム》

```
fx = x^4 + a3*x^3 + a2*x^2 + a1*x + a0;
n = Exponent[fx, x];
RelationsOfX[fx];
For[i = 1, i <= n, i++,
  Print["r[" , i, "] = ", r[i]]
];
```

ここで

```
Exponent[f, x] : xの多項式fについて, xの次数を求める。
とくに,  $f \neq 0$  (定数) の次数は0,  $f = 0$  の次数は $-\infty$ である。
```

《計算結果》

```
r[1] = a0 + a1 X[1] + a2 X[1]^2 + a3 X[1]^3 + X[1]^4
r[2] = a1 + a2 X[1] + a3 X[1]^2 + X[1]^3 + a2 X[2] + a3 X[1]X[2] + X[1]^2X[2] + a3 X[2]^2 + X[1]X[2]^2 + X[2]^3
r[3] = a2 + a3 X[1] + X[1]^2 + a3 X[2] + X[1]X[2] + X[2]^2 + a3 X[3] + X[1]X[3] + X[2]X[3] + X[3]^2
r[4] = a3 + X[1] + X[2] + X[3] + X[4]
```

2. $x_1, x_2, \dots, x_n$ からなる多項式の次数低減

$x_1, x_2, \dots, x_n$ からなる多項式が与えられたとき、根 $x_1, x_2, \dots, x_n$ の関係式 $r_1=0, r_2=0, \dots, r_n=0$ を使えば、 x_1 の次数は $n-1$ 以下に、 x_2 の次数は $n-2$ 以下に、そして x_{n-1} の次数は1以下に低減し、 x_n は消去することができる。 $x_1, x_2, \dots, x_n$ からなる多項式を P とし、以下にその方法を示す。まず、 P と r_n を x_n の多項式と見て、 P の r_n による剰余を改めて P とすれば、 r_n は x_n の1次多項式であるから、 P 中の x_n が消去される。この P と r_{n-1} を x_{n-1} の多項式と見て、 P の r_{n-1} による剰余を改めて P とすれば、 r_{n-1} は x_{n-1} の2次多項式であるから、 P 中の x_{n-1} の2次以上の項が消去される。この P と r_{n-2} を x_{n-2} の多項式と見て、 P の r_{n-2} による剰余を改めて P とすれば、 r_{n-2} は x_{n-2} の3次多項式であるから、 P 中の x_{n-2} の3次以上の項が消去される。同様にして、最後は P と r_1 を x_1 の多項式と見て、 P の r_1 による剰余を改めて P とすれば、 r_1 は x_1 の n 次多項式であるから、 P 中の x_1 の n 次以上の項が消去される。とくに、もとの P が $x_1, x_2, \dots, x_n$ の対称式の場合は定数項だけとなる。

(例1) $f(x)=x^4+2x^3+3x^2+4x+5$, $P=x_1^4+x_2^3+x_3^2+x_4$ の場合

(1. 9) より $r_4=x_1+x_2+x_3+x_4+2$ である。 P と r_4 を x_4 の多項式と見て、 P の r_4 による剰余を改めて P とすれば、 P 中の x_4 が消去される。

$$P=x_1^4-x_1+x_2^3-x_2+x_3^2-x_3-2 \quad (2. 1)$$

(1. 7) より $r_3=x_1^2+x_1x_2+x_1x_3+x_2^2+x_2x_3+x_3^2+2(x_1+x_2+x_3)+3$ である。 P と r_3 を x_3 の多項式と見て、 P の r_3 による剰余を改めて P とすれば、 P 中の x_3 の2次以上の項が消去される。

$$P=x_1^4-x_1^2-x_1x_2-x_1x_3-3x_1+x_2^3-x_2^2-x_2x_3-3x_2-3x_3-5 \quad (2. 2)$$

(1. 5) より $r_2=x_1^3+x_1^2x_2+x_1x_2^2+x_2^3+2(x_1^2+x_1x_2+x_2^2)+3(x_1+x_2)+4$ である。 P と r_2 を x_2 の多項式と見て、 P の r_2 による剰余を改めて P とすれば、 P 中の x_2 の3次以上の項が消去される。

$$P=x_1^4-x_1^3-x_1^2x_2-3x_1^2-x_1x_2^2-3x_1x_2-x_1x_3-6x_1-3x_2^2-x_2x_3-6x_2-3x_3-9 \quad (2. 3)$$

(1. 3) より $r_1=x_1^4+2x_1^3+3x_1^2+4x_1+5$ である。 P と r_1 を x_1 の多項式と見て、 P の r_1 による剰余を改めて P とすれば、 P 中の x_1 の4次以上の項が消去される。

$$P=-3x_1^3-x_1^2x_2-6x_1^2-x_1x_2^2-3x_1x_2-x_1x_3-10x_1-3x_2^2-x_2x_3-6x_2-3x_3-14 \quad (2. 4)$$

以上より、 P 中の x_1 は3次以下に、 x_2 は2次以下に、 x_3 は1次以下に低減され、 x_4 は消去される。

(例2) $f(x)=x^4+2x^3+3x^2+4x+5$, $P=x_1^4+x_2^4+x_3^4+x_4^4$ の場合

P と r_4 を x_4 の多項式と見て、 P の r_4 による剰余を改めて P とすれば、 P 中の x_4 が消去される。

$$\begin{aligned} P= & 2x_1^4+4x_1^3x_2+4x_1^3x_3+8x_1^3+6x_1^2x_2^2+12x_1^2x_2x_3+24x_1^2x_2+6x_1^2x_3^2+24x_1^2x_3+24x_1^2+4x_1x_2^3+12x_1x_2^2x_3 \\ & +24x_1x_2^2+12x_1x_2x_3^2+48x_1x_2x_3+48x_1x_2+4x_1x_3^3+24x_1x_3^2+48x_1x_3+32x_1+2x_2^4+4x_2^3x_3+8x_2^3 \\ & +6x_2^2x_3^2+24x_2^2x_3+24x_2^2+4x_2x_3^3+24x_2x_3^2+48x_2x_3+32x_2+2x_3^4+8x_3^3+24x_3^2+32x_3+16 \end{aligned} \quad (2. 5)$$

P と r_3 を x_3 の多項式と見て、 P の r_3 による剰余を改めて P とすれば、 P 中の x_3 の2次以上の項が消去される。ただし本例では、 P は x_3, x_4 の対称式であるため、 P 中の x_3 は消去されて、 P は x_1, x_2 だけの多項式となる。

$$P=-4x_1^3x_2-8x_1^3-4x_1^2x_2^2-16x_1^2x_2-16x_1^2-4x_1x_2^3-16x_1x_2^2-28x_1x_2-24x_1-8x_2^3-16x_2^2-24x_2-14 \quad (2. 6)$$

P と r_2 を x_2 の多項式と見て、 P の r_2 による剰余を改めて P とすれば、 P 中の x_2 の3次以上の項が消去される。ただし本例では、 P は x_2, x_3, x_4 の対称式であるため、 P 中の x_2 は消去されて、 P は x_1 だけの多項式となる。

$$P=4x_1^4+8x_1^3+12x_1^2+16x_1+18 \quad (2. 7)$$

P と r_1 を x_1 の多項式と見て、 P の r_1 による剰余を改めて P とすれば、 P 中の x_1 の4次以上の項が消去される。ただし本例では、 P は x_1, x_2, x_3, x_4 の対称式であるため、 P 中の x_1 は消去されて、 P は定数項だけとなる。

$$P=-2 \quad (2.8)$$

P が x_1, x_2, x_3, x_4 の対称式の場合は、 P 中の x_1, x_2, x_3, x_4 は消去されて、 P は定数項だけになることはよく知られている。そうでない場合であっても、 P が x_2, x_3, x_4 の対称式ならば、 P 中の x_2, x_3, x_4 は消去されて、 P は x_1 だけの多項式になる。 P が x_3, x_4 の対称式ならば、 P 中の x_3, x_4 は消去されて、 P は x_1, x_2 だけの多項式になる。次節で述べる $g(x)$ の計算方法の改良は、これに基づいて考え出された。

数式処理ソフトによる計算

《サブプログラム》

$X[1], X[2], \dots, X[n]$ からなる多項式の次数を低減する。

(* Reduction of $X[1], X[2], \dots, X[n]$ *)

ReductionOfX[P_] := Module[{i, Q},

Q=P;

For[i=n, i>=1, i--,

Q=PolynomialRemainder[Q, r[i], X[i]]

];

Return[Expand[Simplify[Q]]]

];

ここで

Return[x] : 戻り値をxとし、関数から抜け出す。

Expand[f] : 数式fを展開する。

Simplify[f] : 数式fを簡略する。

《メインプログラム》

fx=x^4+2*x^3+3*x^2+4*x+5;

n=Exponent[fx, x];

RelationsOfX[fx];

P=X[1]^4+X[2]^3+X[3]^2+X[4];

Print["P=", ReductionOfX[P]];

P=X[1]^4+X[2]^4+X[3]^4+X[4]^4;

Print["P=", ReductionOfX[P]];

《計算結果》

P=-14-10X[1]-6X[1]^2-3X[1]^3-6X[2]-3X[1]X[2]-X[1]^2X[2]-3X[2]^2-X[1]X[2]^2-3X[3]-X[1]X[3]-X[2]X[3]

P=-2

3. $x_1, x_2, \dots, x_n$ の置換 $\sigma_1, \sigma_2, \dots, \sigma_{n!}$

$x_1, x_2, \dots, x_n$ を $x_{j_1}, x_{j_2}, \dots, x_{j_n}$ ($j_1, j_2, \dots, j_n$ は $1, 2, \dots, n$ を並べ替えたもの)に移す $n!$ 通りの置換を $\sigma_1, \sigma_2, \dots, \sigma_{n!}$ とする。ここで、 $n!$ 通りの $j_1, j_2, \dots, j_n$ は j_1 の小さい順、 j_1 が同じならば j_2 の小さい順、 j_1, j_2 が同じならば j_3 の小さい順、そして $j_1, j_2, \dots, j_{n-2}$ が同じならば j_{n-1} の小さい順に並べるものとする。

(例) $n=4$ の場合

$\sigma_i (i=1, 2, \dots, 24)$ について、 i と j_1, j_2, j_3, j_4 の対応表を示す。

i	j_1	j_2	j_3	j_4
1	1	2	3	4
2	1	2	4	3
3	1	3	2	4
4	1	3	4	2
5	1	4	2	3
6	1	4	3	2
7	2	1	3	4
8	2	1	4	3

i	j_1	j_2	j_3	j_4
9	2	3	1	4
10	2	3	4	1
11	2	4	1	3
12	2	4	3	1
13	3	1	2	4
14	3	1	4	2
15	3	2	1	4
16	3	2	4	1

i	j_1	j_2	j_3	j_4
17	3	4	1	2
18	3	4	2	1
19	4	1	2	3
20	4	1	3	2
21	4	2	1	3
22	4	2	3	1
23	4	3	1	2
24	4	3	2	1

数式処理ソフトによる計算

《プログラム》

```
n=4;
sigma=Permutations[Table[i, {i, 1, n}]];
Print["sigma=", sigma];
```

ここで

Permutations[v] : 配列v中の要素を並べ替えた2次元配列を作る。

Table[f, {i, i1, i2}] : i=i1からi=i2まで、数式fの配列を作る。

《計算結果》

```
sigma={ {1, 2, 3, 4}, {1, 2, 4, 3}, {1, 3, 2, 4}, {1, 3, 4, 2}, {1, 4, 2, 3}, {1, 4, 3, 2},
  {2, 1, 3, 4}, {2, 1, 4, 3}, {2, 3, 1, 4}, {2, 3, 4, 1}, {2, 4, 1, 3}, {2, 4, 3, 1},
  {3, 1, 2, 4}, {3, 1, 4, 2}, {3, 2, 1, 4}, {3, 2, 4, 1}, {3, 4, 1, 2}, {3, 4, 2, 1},
  {4, 1, 2, 3}, {4, 1, 3, 2}, {4, 2, 1, 3}, {4, 2, 3, 1}, {4, 3, 1, 2}, {4, 3, 2, 1} }
```


4. 原始要素 v とその最小多項式 $g(x)$

$m_1, m_2, \dots, m_n$ は相異なる整数とし

$$v = m_1 x_1 + m_2 x_2 + \dots + m_n x_n \quad (4.1)$$

とする。右辺の $x_1, x_2, \dots, x_n$ を $\sigma_1, \sigma_2, \dots, \sigma_n!$ で置換したものを $v_1, v_2, \dots, v_n!$ とする。これらが相異なる値となるように $m_1, m_2, \dots, m_n$ を決めれば、 v は $f(x)$ の分解体の原始要素となる。これには

$$g(x) = (x-v_1)(x-v_2)\cdots(x-v_n!) \quad (4.2)$$

としたとき —— これは $x_1, x_2, \dots, x_n$ の対称式であるから、根 $x_1, x_2, \dots, x_n$ の関係式を用いると $x_1, x_2, \dots, x_n$ は消去され、その係数は $a_{n-1}, \dots, a_1, a_0$ の多項式となる。—— これが重根を持たなければ、すなわち $g(x)$ と $g'(x)$ が互いに素であればよい。 $m_1, m_2, \dots, m_n$ は1, -1, 2, -2, 3, -3, $\dots$ の順に試行し、以下のように決めていく。まず、 $m_1=1$ に決める。 $m_2 \neq 0$, $m_3 = \dots = m_n = 0$ とすると、 $v_1, v_2, \dots, v_n!$ は $(n-2)!$ 個ずつ同じ式が連続して現れるので($\sigma_1, \sigma_2, \dots, \sigma_n!$ がそのような順序に並べられている)、 $v_1, v_2, \dots, v_n!$ の中から $(n-2)!$ 個毎に、計 $n(n-1)$ 個の v_i を取り出して、これらがすべて異なる値となるように m_2 を決める。つぎに、 $m_3 \neq 0$ とすると、 $v_1, v_2, \dots, v_n!$ は $(n-3)!$ 個ずつ同じ式が連続して現れるので、 $v_1, v_2, \dots, v_n!$ の中から $(n-3)!$ 個毎に、計 $n(n-1)(n-2)$ 個の v_i を取り出して、これらがすべて異なる値となるように m_3 を決める。同様にして、最後は $m_{n-1} \neq 0$ とすると、 $v_1, v_2, \dots, v_n!$ はすべて異なる式となるので、これらがすべて異なる値となるように m_{n-1} を決める。この $m_1, m_2, \dots, m_{n-1}$ により、 $v_1, v_2, \dots, v_n!$ はすべて異なる値となるので、残りは $m_n=0$ としてよい。このとき、 $g(x)$ を有理係数の範囲で因数分解し、任意の1因数を改めて $g(x)$ とすれば、これが v の最小多項式となる。

(例1) $n=5$ の場合

(1) $m_1=1$ とする。 $m_3=m_4=m_5=0$ とし、 $m_2=-1, 2, -2, 3, -3, \dots$ の順に試行して、3!個毎に取り出した計20個の $x-v_i$ の積 $g(x)=(x-v_1)(x-v_7)\cdots(x-v_{115})$ と $g'(x)$ が互いに素であるように m_2 を決める。

(2) $m_4=m_5=0$ とし、 $m_3=2, -2, 3, -3, \dots$ の順に試行して、2!個毎に取り出した計60個の $x-v_i$ の積 $g(x)=(x-v_1)(x-v_3)\cdots(x-v_{119})$ と $g'(x)$ が互いに素であるように m_3 を決める。

(3) $m_5=0$ とし、 $m_4=-2, 3, -3, \dots$ の順に試行して、 $g(x)=(x-v_1)(x-v_2)\cdots(x-v_{120})$ と $g'(x)$ が互いに素であるように m_4 を決める。残りは $m_5=0$ とする。

(例2) $f(x)=x^3+a_2x^2+a_1x+a_0$ の場合

$m_1=1, m_2=-1, m_3=0$ とすると、 $g(x)$ は次式となる。

$$\begin{aligned} g(x) &= (x-v_1)(x-v_2)(x-v_3)(x-v_4)(x-v_1)(x-v_6) \\ &= (x-x_1+x_2)(x-x_1+x_3)(x-x_2+x_1)(x-x_2+x_3)(x-x_3+x_1)(x-x_3+x_2) \\ &= x^6 + 2\{-(x_1^2+x_2^2+x_3^2) + (x_1x_2+x_1x_3+x_2x_3)\}x^4 + \{(x_1^4+x_2^4+x_3^4) - 2(x_1^3x_2+x_1^3x_3+x_1x_2^3+x_1x_3^3+x_2^3x_3+x_2x_3^3) \\ &\quad + 3(x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2)\}x^2 - (x_1^4x_2^2+x_1^4x_3^2+x_1^2x_2^4+x_1^2x_3^4+x_2^4x_3^2+x_2^2x_3^4) + 2x_1x_2x_3(x_1^3+x_2^3+x_3^3) \\ &\quad + 2(x_1^3x_2^3+x_1^3x_3^3+x_2^3x_3^3) - 2x_1x_2x_3(x_1^2x_2+x_1^2x_3+x_1x_2^2+x_1x_3^2+x_2^2x_3+x_2x_3^2) + 6x_1^2x_2^2x_3^2 \\ &= x^6 + 2(3a_1-a_2^2)x^4 + (9a_1^2-6a_1a_2^2+a_2^4)x^2 + 27a_0^2+4a_1^3-18a_0a_1a_2-a_1^2a_2^2+4a_0a_2^3 \end{aligned} \quad (4.3)$$

この $g(x)$ は既約であるから、これが v の最小多項式である。

(例3) $f(x)=x^4+a_2x^2+a_0$ の場合

(1) $m_1=1, m_2=-1, m_3=0, m_4=0$ とすると, $g(x)$ は次式となる。

$$\begin{aligned} g(x) &= (x-v_1)(x-v_3)\cdots(x-v_{23}) \\ &= x^{12}+8a_2x^{10}+2(4a_0+11a_2^2)x^8+4a_2(4a_0+7a_2^2)x^6-(112a_0^2-24a_0a_2^2-17a_2^4)x^4 \\ &\quad -4a_2(4a_0-a_2^2)(12a_0+a_2^2)x^2+16a_0(4a_0-a_2^2)^2 \end{aligned} \quad (4.4)$$

$g(x)$ と $g'(x)$ は互いに素ではないから(共通因数は $x^4+2a_2x^2-4a_0+a_2^2$), $m_2=-1$ は不適当である。

(2) $m_1=1, m_2=2, m_3=0, m_4=0$ とすると, $g(x)$ は次式となる。

$$\begin{aligned} g(x) &= (x-v_1)(x-v_3)\cdots(x-v_{23}) \\ &= x^{12}+11a_2x^{10}-(13a_0-43a_2^2)x^8-a_2(74a_0-73a_2^2)x^6+(611a_0^2-237a_0a_2^2+56a_2^4)x^4 \\ &\quad +a_2(555a_0^2-160a_0a_2^2+16a_2^4)x^2+a_0(25a_0-4a_2^2)^2 \end{aligned} \quad (4.5)$$

$g(x)$ と $g'(x)$ は互いに素であるから, $m_2=2$ に決める。

(3) $m_1=1, m_2=2, m_3=-2, m_4=0$ とすると, $g(x)$ は次式となる。

$$\begin{aligned} g(x) &= (x-v_1)(x-v_2)\cdots(x-v_{24}) \\ &= x^{24}+70a_2x^{22}+7(10a_0+297a_2^2)x^{20}+10a_2(259a_0+3450a_2^2)x^{18}+7(4985a_0^2+3092a_0a_2^2+50745a_2^4)x^{16} \\ &\quad +70a_2(17034a_0^2-3734a_0a_2^2+34065a_2^4)x^{14}-(11125100a_0^3-20712058a_0^2a_2^2+6532546a_0a_2^4 \\ &\quad -10674705a_2^6)x^{12}-70a_2(3164470a_0^3-2901946a_0^2a_2^2+798335a_0a_2^4-457320a_2^6)x^{10} \\ &\quad +7(365305145a_0^4-408311100a_0^3a_2^2+184160985a_0^2a_2^4-37215568a_0a_2^6+9090720a_2^8)x^8 \\ &\quad +10a_2(2655833507a_0^4-1839114654a_0^3a_2^2+518070512a_0^2a_2^4-72189632a_0a_2^6 \\ &\quad +8168320a_2^8)x^6-7(5724579062a_0^5-16082653801a_0^4a_2^2+8170093984a_0^3a_2^4 \\ &\quad -1692817088a_0^2a_2^6+166114048a_0a_2^8-9217792a_2^{10})x^4-70a_2(3296792031a_0^5 \\ &\quad -3432644488a_0^4a_2^2+1222395456a_0^3a_2^4-192242304a_0^2a_2^6+13710592a_0a_2^8-405504a_2^{10})x^2 \\ &\quad +(25a_0-4a_2^2)^2(169a_0-36a_2^2)^2(289a_0-16a_2^2)^2 \end{aligned} \quad (4.6)$$

$g(x)$ と $g'(x)$ は互いに素であるから, $m_3=-2$ に決める。

(4) $g(x)$ を因数分解すると次式となる。

$$\begin{aligned} g(x) &= \{x^8+10a_2x^6-(14a_0-33a_2^2)x^4-10a_2(7a_0-4a_2^2)x^2+(25a_0-4a_2^2)^2\} \\ &\quad \times \{x^8+26a_2x^6-(238a_0-241a_2^2)x^4-26a_2(119a_0-36a_2^2)x^2+(169a_0-36a_2^2)^2\} \\ &\quad \times \{x^8+34a_2x^6+(322a_0+321a_2^2)x^4+34a_2(161a_0+16a_2^2)x^2+(289a_0-16a_2^2)^2\} \end{aligned} \quad (4.7)$$

右辺の任意の1因数を改めて $g(x)$ とすれば, これが v の最小多項式となる。例えば, 右辺の1番目の因数を取ると, $g(x)$ は次式となる。

$$g(x)=x^8+10a_2x^6-(14a_0-33a_2^2)x^4-10a_2(7a_0-4a_2^2)x^2+(25a_0-4a_2^2)^2 \quad (4.8)$$

《 $g(x)$ の計算方法の改良》

$g(x)$ の計算方法については、 $x-v_i$ を $i=1, 2, \dots, n!$ の順に掛けていくのではなく、 $x-v_i$ の順序を適当に並べ替え、 $x_1, x_2, \dots, x_n$ の対称性を利用することにより、 $g(x)$ の計算時間を短縮することができる。これを $n=4$ の場合について、下図を用いて説明する。

$$\begin{array}{lcl}
 x-v_1=x-(m_1x_1+m_2x_2+m_3x_3+m_4x_4) & \left. \vphantom{\begin{array}{l} x-v_1 \\ x-v_2 \\ x-v_3 \\ x-v_4 \\ x-v_5 \\ x-v_6 \\ x-v_7 \\ x-v_8 \\ x-v_{13} \\ x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{11}(x) & \left. \vphantom{\begin{array}{l} g_{11}(x) \\ g_{12}(x) \\ g_{13}(x) \end{array}} \right\} g_{21}(x) \\
 x-v_2=x-(m_1x_1+m_2x_2+m_4x_3+m_3x_4) & \left. \vphantom{\begin{array}{l} x-v_2 \\ x-v_3 \\ x-v_4 \\ x-v_5 \\ x-v_6 \\ x-v_7 \\ x-v_8 \\ x-v_{13} \\ x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{12}(x) & \\
 x-v_3=x-(m_1x_1+m_3x_2+m_2x_3+m_4x_4) & \left. \vphantom{\begin{array}{l} x-v_3 \\ x-v_4 \\ x-v_5 \\ x-v_6 \\ x-v_7 \\ x-v_8 \\ x-v_{13} \\ x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{13}(x) & \\
 x-v_4=x-(m_1x_1+m_4x_2+m_2x_3+m_3x_4) & \left. \vphantom{\begin{array}{l} x-v_4 \\ x-v_5 \\ x-v_6 \\ x-v_7 \\ x-v_8 \\ x-v_{13} \\ x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{14}(x) & \\
 x-v_5=x-(m_1x_1+m_4x_2+m_3x_3+m_2x_4) & \left. \vphantom{\begin{array}{l} x-v_5 \\ x-v_6 \\ x-v_7 \\ x-v_8 \\ x-v_{13} \\ x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{15}(x) & \\
 x-v_6=x-(m_2x_1+m_1x_2+m_3x_3+m_4x_4) & \left. \vphantom{\begin{array}{l} x-v_6 \\ x-v_7 \\ x-v_8 \\ x-v_{13} \\ x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{16}(x) & \\
 x-v_7=x-(m_2x_1+m_1x_2+m_4x_3+m_3x_4) & \left. \vphantom{\begin{array}{l} x-v_7 \\ x-v_8 \\ x-v_{13} \\ x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{17}(x) & \\
 x-v_{13}=x-(m_2x_1+m_3x_2+m_1x_3+m_4x_4) & \left. \vphantom{\begin{array}{l} x-v_{13} \\ x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{18}(x) & \\
 x-v_{19}=x-(m_2x_1+m_3x_2+m_4x_3+m_1x_4) & \left. \vphantom{\begin{array}{l} x-v_{19} \\ x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{19}(x) & \\
 x-v_{14}=x-(m_2x_1+m_4x_2+m_1x_3+m_3x_4) & \left. \vphantom{\begin{array}{l} x-v_{14} \\ x-v_{20} \end{array}} \right\} g_{110}(x) & \\
 x-v_{20}=x-(m_2x_1+m_4x_2+m_3x_3+m_1x_4) & \left. \vphantom{\begin{array}{l} x-v_{20} \end{array}} \right\} g_{111}(x) & \\
 x-v_9=x-(m_3x_1+m_1x_2+m_2x_3+m_4x_4) & \left. \vphantom{\begin{array}{l} x-v_9 \\ x-v_{11} \\ x-v_{15} \\ x-v_{21} \\ x-v_{17} \\ x-v_{23} \end{array}} \right\} g_{112}(x) & \\
 x-v_{11}=x-(m_3x_1+m_1x_2+m_4x_3+m_2x_4) & \left. \vphantom{\begin{array}{l} x-v_{11} \\ x-v_{15} \\ x-v_{21} \\ x-v_{17} \\ x-v_{23} \end{array}} \right\} g_{113}(x) & \\
 x-v_{15}=x-(m_3x_1+m_2x_2+m_1x_3+m_4x_4) & \left. \vphantom{\begin{array}{l} x-v_{15} \\ x-v_{21} \\ x-v_{17} \\ x-v_{23} \end{array}} \right\} g_{114}(x) & \\
 x-v_{21}=x-(m_3x_1+m_2x_2+m_4x_3+m_1x_4) & \left. \vphantom{\begin{array}{l} x-v_{21} \\ x-v_{17} \\ x-v_{23} \end{array}} \right\} g_{115}(x) & \\
 x-v_{17}=x-(m_3x_1+m_4x_2+m_1x_3+m_2x_4) & \left. \vphantom{\begin{array}{l} x-v_{17} \\ x-v_{23} \end{array}} \right\} g_{116}(x) & \\
 x-v_{23}=x-(m_3x_1+m_4x_2+m_2x_3+m_1x_4) & \left. \vphantom{\begin{array}{l} x-v_{23} \end{array}} \right\} g_{117}(x) & \\
 x-v_{10}=x-(m_4x_1+m_1x_2+m_2x_3+m_3x_4) & \left. \vphantom{\begin{array}{l} x-v_{10} \\ x-v_{12} \\ x-v_{16} \\ x-v_{22} \\ x-v_{18} \end{array}} \right\} g_{118}(x) & \\
 x-v_{12}=x-(m_4x_1+m_1x_2+m_3x_3+m_2x_4) & \left. \vphantom{\begin{array}{l} x-v_{12} \\ x-v_{16} \\ x-v_{22} \\ x-v_{18} \end{array}} \right\} g_{119}(x) & \\
 x-v_{16}=x-(m_4x_1+m_2x_2+m_1x_3+m_3x_4) & \left. \vphantom{\begin{array}{l} x-v_{16} \\ x-v_{22} \\ x-v_{18} \end{array}} \right\} g_{120}(x) & \\
 x-v_{22}=x-(m_4x_1+m_2x_2+m_3x_3+m_1x_4) & \left. \vphantom{\begin{array}{l} x-v_{22} \\ x-v_{18} \end{array}} \right\} g_{121}(x) & \\
 x-v_{18}=x-(m_4x_1+m_3x_2+m_1x_3+m_2x_4) & \left. \vphantom{\begin{array}{l} x-v_{18} \end{array}} \right\} g_{122}(x) & \\
 x-v_{24}=x-(m_4x_1+m_3x_2+m_2x_3+m_1x_4) & \left. \vphantom{\begin{array}{l} x-v_{24} \end{array}} \right\} g_{123}(x) &
 \end{array}
 \left. \vphantom{\begin{array}{l} g_{11}(x) \\ g_{12}(x) \\ g_{13}(x) \\ g_{14}(x) \\ g_{15}(x) \\ g_{16}(x) \\ g_{17}(x) \\ g_{18}(x) \\ g_{19}(x) \\ g_{110}(x) \\ g_{111}(x) \\ g_{112}(x) \\ g_{113}(x) \\ g_{114}(x) \\ g_{115}(x) \\ g_{116}(x) \\ g_{117}(x) \\ g_{118}(x) \\ g_{119}(x) \\ g_{120}(x) \\ g_{121}(x) \\ g_{122}(x) \\ g_{123}(x) \end{array}} \right\} g(x)$$

- (1) $x-v$ を $\sigma_1, \sigma_2, \dots, \sigma_{24}$ で置換する代わりに $\sigma_1^{-1}, \sigma_2^{-1}, \dots, \sigma_{24}^{-1}$ で置換する。これを上図の第1列に示す。これは x_1, x_2, x_3, x_4 の代わりに m_1, m_2, m_3, m_4 を $\sigma_1, \sigma_2, \dots, \sigma_{24}$ で置換するのと同じである。なぜならば、さらに x_1, x_2, x_3, x_4 を $\sigma_1, \sigma_2, \dots, \sigma_{24}$ で置換すると、もとに戻るからである。このようにすると、 x_1 の係数が m_1, m_2, m_3, m_4 の順に並ぶ。 x_1 の係数が同じ場合は、 x_2 の係数が m_1, m_2, m_3, m_4 の順に並ぶ。そして、 x_1, x_2 の係数が同じ場合は、 x_3 の係数が m_1, m_2, m_3, m_4 の順に並ぶ。
- (2) 第1列の $x-v_i$ ($i=1, 2, \dots, 24$)を2個ずつ取って掛け合わせ、第2節で述べた方法により x_1, x_2, x_3, x_4 の次数を低減させて、その結果を第2列の $g_{1k}(x)$ ($k=1, 2, \dots, 12$)とする。このとき、 $g_{1k}(x)$ は x_3, x_4 の対称式であるから、 x_1, x_2 だけが残る。
- (3) 第2列の $g_{1k}(x)$ ($k=1, 2, \dots, 12$)を3個ずつ取って掛け合わせ、第2節で述べた方法により x_1, x_2, x_3, x_4 の次数を低減させて、その結果を第3列の $g_{2l}(x)$ ($l=1, 2, 3, 4$)とする。このとき、 $g_{1k}(x)$ は x_1, x_2 だけからなるので、 x_3, x_4 の次数低減は省略することができる。 $g_{2l}(x)$ は x_2, x_3, x_4 の対称式であるから、 x_1 だけが残る。
- (4) 第3列の $g_{2l}(x)$ ($l=1, 2, 3, 4$)を掛け合わせ、第2節で述べた方法により x_1, x_2, x_3, x_4 の次数を低減させて、その結果を第4列の $g(x)$ とする。このとき、 $g_{2l}(x)$ は x_1 だけからなるので、 x_2, x_3, x_4 の次数低減は省略することができる。 $g(x)$ は x_1, x_2, x_3, x_4 の対称式であるから、定数項だけとなる。

以下に、Cプログラム風にしたアルゴリズムを示す。ただし、 $g_{ik}(x)$ ($k=4, 5, \dots, 12$) の記憶場所は $g_{ik}(x)$ ($k=1, 2, 3$) の記憶場所と共有した。

```

i=0;
for (l=1; l<=4; l++) {
  for (k=1; k<=3; k++) {
    for (j=1; j<=2; j++) {
      i++;
       $v$ 中の $m_1, m_2, m_3, m_4$ を $\sigma_i$ で置換したものを $v_i$ とする。
      if (j==1) { $g_{1k}(x)=x-v_i$ ; continue;}
       $g_{1k}(x)=(x-v_i)g_{1k}(x)$  とし、 $x_1, x_2, x_3, x_4$ の次数を低減させる。
    }
    if (k==1) { $g_{2l}(x)=g_{1k}(x)$ ; continue;}
     $g_{2l}(x)=g_{1k}(x)g_{2l}(x)$  とし、 $x_1, x_2$ の次数を低減させる。
  }
  if (l==1) { $g(x)=g_{2l}(x)$ ; continue;}
   $g(x)=g_{2l}(x)g(x)$  とし、 $x_1$ の次数を低減させる。
}

```

これを一般の n の場合のアルゴリズムに書き換える。 $n=4$ の場合の j, k, l を変数とする3重の反復計算は、一般の n の場合には $n-1$ 重の反復計算となるが、変数を配列 $c[j]$ ($j=1, 2, \dots, n-1$)に変更して、その値を $\{1, 1, \dots, 1\}$ から $\{2, 3, \dots, n\}$ まで逐次更新すれば、単一の反復計算として書くことができる。これより、一般の n の場合のアルゴリズムは以下ようになる。

```

i=0;
for (j=1; j<=n-1; j++) c[j]=1;
while(true) {
  for (j=1; j<=n-1; j++) {
    if (j==1) {
      i++;
       $v$ 中の $m_1, m_2, \dots, m_n$ を $\sigma_i$ で置換したものを $v_i$ とする。
      if (c[j]==1) {
         $g_{j, c[j+1]}(x)=x-v_i$ ;
      }
      else {
         $g_{j, c[j+1]}(x)=(x-v_i)g_{j, c[j+1]}(x)$  とし、 $x_1, x_2, \dots, x_n$ の次数を低減させる。
      }
    }
    else if (j<=n-2) {
      if (c[j]==1) {
         $g_{j, c[j+1]}(x)=g_{j-1, c[j]}(x)$ ;
      }
      else {
         $g_{j, c[j+1]}(x)=g_{j-1, c[j]}(x)g_{j, c[j+1]}(x)$  とし、 $x_1, x_2, \dots, x_{n-j}$ の次数を低減させる。
      }
    }
  }
  else {

```

```

    if (c[j]==1) {
         $g(x)=g_{j-1, c[j]}(x)$ ;
    }
    else{
         $g(x)=g_{j-1, c[j]}(x)g(x)$  とし,  $x_1$  の次数を低減させる。
    }
}
if (c[j]<=j) break;
}
for (j=1; j<=n-1; j++) {
    if (c[j]<j+1) {
        c[j]++; break;
    }
    else{
        c[j]=1;
    }
}
if (i==n!) break;
}

```

これで完成ではない。このアルゴリズムは、前もって $m_1, m_2, \dots, m_n$ の値が決められている場合のものである。実際は上述したように、 $m_1=1$, $m_n=0$ とし、残りの $m_k (k=2, 3, \dots, n-1)$ は1つずつ試行しながら決めていく。そして、 m_k を決めるときは、 $x-v_i$ を $(n-k)!$ 個毎に、計 $n!/(n-k)!$ 個だけ取り出して、それらの積を $g(x)$ とする。このようにするために、上記のアルゴリズムの第5-14行を以下のように変更する。第4行の $\text{mod}(l-1, \text{factorial}(n-k))$ は $l-1$ の $(n-k)!$ による剰余を表す。

```

if (j=1) {
    i++;
     $\sigma_i = \sigma_i^{-1}$  となる  $l$  を求める。
    if (mod(l-1, factorial(n-k)) != 0) {
        if (c[j]==1)  $g_{j, c[j+1]}(x)=1$ ;
    }
    else{
         $v$  中の  $m_1, m_2, \dots, m_n$  を  $\sigma_i$  で置換したものを  $v_i$  とする。
        if (c[j]==1) {
             $g_{j, c[j+1]}(x)=x-v_i$ ;
        }
        else{
             $g_{j, c[j+1]}(x)=(x-v_i)g_{j, c[j+1]}(x)$  とし,  $x_1, x_2, \dots, x_n$  の次数を低減させる。
        }
    }
}
}

```

数式処理ソフトによる計算

《サブプログラム》

V[1]が原始要素となるようにm[1], m[2], ..., m[n]を決める。

(* Calculation of m[1], m[2], ..., m[n] *)

```
PrimitiveElement[]:=Module[{c, g, i, j, k, L, p, q, vi},
  For[k=1, k<=n, k++,
    m[k]=If[k==1, 1, 0]
  ];
  Print["m[1]=1"];
  For[k=2, k<=n-1, k++,
    m[k]=If[m[k-1]>0, -m[k-1], 1-m[k-1]];
    While[True,
      i=0;
      For[j=1, j<=n-1, j++, c[j]=1];
      While[True,
        For[j=1, j<=n-1, j++,
          If[j==1,
            i++;
            For[L=1, L<=nn, L++,
              p=Table[Part[sigma, i, Part[sigma, L, q]], {q, 1, n}];
              If[p==Table[q, {q, 1, n}], Break[]]
            ];
            If[Mod[L-1, Factorial[n-k]]!=0,
              If[c[j]==1, g[j, c[j+1]]=1],
              vi=Sum[m[Part[sigma, i, L]]*X[L], {L, 1, n}];
              If[c[j]==1,
                g[j, c[j+1]]=x-vi,
                g[j, c[j+1]]=ReductionOfX[Expand[(x-vi)*g[j, c[j+1]]]]
              ]
            ]
          ];
          If[j>=2 && j<=n-2,
            If[c[j]==1,
              g[j, c[j+1]]=g[j-1, c[j]],
              g[j, c[j+1]]=ReductionOfX[Expand[g[j-1, c[j]]*g[j, c[j+1]]]]
            ]
          ];
          If[j==n-1,
            If[c[j]==1,
              gx=g[j-1, c[j]],
              gx=ReductionOfX[Expand[g[j-1, c[j]]*gx]]
            ]
          ];
          If[c[j]<=j, Break[]]
```

```

];
For[j=1, j<=n-1, j++,
  If[c[j]<j+1,
    c[j]++; Break[],
    c[j]=1
  ]
];
If[i==nn, Break[]]
];
If[Exponent[PolynomialGCD[gx, D[gx, x]], x]==0, Break[]];
m[k]=If[m[k]>0, -m[k], 1-m[k]]
];
Print["m[" , k, "]=", m[k]]
];
Print["m[" , n, "] = 0"];
For[i=1, i<=nn, i++,
  V[i]=Sum[m[L]*X[Part[sigma, i, L]], {L, 1, n}]
]
];

```

ここで

If[t, x, y] : 条件tが真ならばx, 偽ならばyとする。yは省略できる。
 xまたはyが複数の文からなる場合は各文を";"で区切る。xとyの間は", "で区切る。
 While[t, proc] : 条件tが真の間だけ, 手続きprocを反復する。
 procが複数の文からなる場合は各文を";"で区切る。
 Part[v, i] : 配列v中のi番目の要素を求める。
 Break[] : 反復中の手続きから抜け出す。
 Mod[m, n] : mのnによる剰余を求める。
 Factorial[n] : nの階乗を求める。
 Sum[f, {i, i1, i2}] : i=i1からi=i2まで, 数式fの和を求める。
 PolynomialGCD[f, g] : 多項式fとgの最大の共通因数を求める。
 D[f, x] : 数式fのxによる微分を求める。

《サブプログラム(2)》

原始要素V[1]の最小多項式gxを求める。

```
(* Calculation of g(x) *)
MinimalPolynomial[]:=Module[{Gx,i},
  Gx=FactorList[gx];
  If[Length[Gx]==2,Return[]];
  Print["factors of g(x) : "];
  For[i=2,i<=Length[Gx],i++,
    Print["(",i-1,")",Part[Gx,i,1]]
  ];
  i=Input["Select one of factors : "]+1;
  gx=Part[Gx,i,1]
];
```

ここで

FactorList[f] : 多項式fを因数分解し、その結果を配列形式で表す。

因数の数値部分が第1要素に、数式部分が第2要素以降に入れられる。

Length[v] : 配列vの要素数を求める。

Input[prompt] : 入力要求promptを表示して数式を入力する。

《メインプログラム》

```
fx=x^4+a2*x^2+a0;
n=Exponent[fx,x];
nn=Factorial[n];
RelationsOfX[fx];
sigma=Permutations[Table[i,{i,1,n}]];
PrimitiveElement[];
MinimalPolynomial[];
Print["g(x)=",gx];
```

《計算結果》

m[1]=1

m[2]=2

m[3]=-2

m[4]=0

factors of g(x) :

(1) $625a_0^2 - 200a_0 a_2^2 + 16a_2^4 - 70a_0 a_2 x^2 + 40a_2^3 x^2 - 14a_0 x^4 + 33a_2^2 x^4 + 10a_2 x^6 + x^8$

(2) $28561a_0^2 - 12168a_0 a_2^2 + 1296a_2^4 - 3094a_0 a_2 x^2 + 936a_2^3 x^2 - 238a_0 x^4 + 241a_2^2 x^4 + 26a_2 x^6 + x^8$

(3) $83521a_0^2 - 9248a_0 a_2^2 + 256a_2^4 + 5474a_0 a_2 x^2 + 544a_2^3 x^2 + 322a_0 x^4 + 321a_2^2 x^4 + 34a_2 x^6 + x^8$

入力要求"Select one of factors : "に対して"1"を入力する(1番目の因数を選ぶ)と

$g(x) = 625a_0^2 - 200a_0 a_2^2 + 16a_2^4 - 70a_0 a_2 x^2 + 40a_2^3 x^2 - 14a_0 x^4 + 33a_2^2 x^4 + 10a_2 x^6 + x^8$

5. $f(x)$ の分解体の基底 $w_1, w_2, \dots, w_{n!}$

第2節によると, $f(x)$ の分解体の元は以下に示す $n!$ 個の基底 $w_1, w_2, \dots, w_{n!}$ の1次式で表される。

$$w_i = x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} \quad (0 \leq j_1 \leq n-1, 0 \leq j_2 \leq n-2, \dots, 0 \leq j_{n-1} \leq 1, j_n = 0) \quad (5.1)$$

ここで, $n!$ 通りの $j_1, j_2, \dots, j_n$ は j_1 の小さい順, j_1 が同じならば j_2 の小さい順, j_1, j_2 が同じならば j_3 の小さい順, そして $j_1, j_2, \dots, j_{n-2}$ が同じならば j_{n-1} の小さい順に並べるものとする。

(追記) $g(x)$ の次数が $n!$ より小さい場合は, $f(x)$ の分解体の基底になるのは $w_1, w_2, \dots, w_{n!}$ の一部だけであるが, この場合も今後の議論の支障にはならないので, そのまま進めることにする。

(例) $n=4$ の場合

$w_i (i=1, 2, \dots, 24)$ について, i と j_1, j_2, j_3, j_4 の対応表を示す。

i	j_1	j_2	j_3	j_4
1	0	0	0	0
2	0	0	1	0
3	0	1	0	0
4	0	1	1	0
5	0	2	0	0
6	0	2	1	0
7	1	0	0	0
8	1	0	1	0

i	j_1	j_2	j_3	j_4
9	1	1	0	0
10	1	1	1	0
11	1	2	0	0
12	1	2	1	0
13	2	0	0	0
14	2	0	1	0
15	2	1	0	0
16	2	1	1	0

i	j_1	j_2	j_3	j_4
17	2	2	0	0
18	2	2	1	0
19	3	0	0	0
20	3	0	1	0
21	3	1	0	0
22	3	1	1	0
23	3	2	0	0
24	3	2	1	0

数式処理ソフトによる計算

《サブプログラム》

分解体の基底 $w[1], w[2], \dots, w[n!]$ を求める。

(* Calculation of $w[1], w[2], \dots, w[n!]$ *)

```
BasisOfSplittingField[]:=Module[{i, j, wi},
  w={};
  For[i=1, i<=nn, i++,
    wi={};
    For[j=1, j<=n, j++,
      AppendTo[wi, Mod[Floor[(i-1)/Factorial[n-j]], n-j+1]]];
    AppendTo[w, wi]
  ]
];
```

ここで

AppendTo[v, x] : 配列vにxを追加する。

Floor[x] : x以下の最大の整数を求める。

《メインプログラム》

```
n=4;  
nn=Factorial[n];  
BasisOfSplittingField[];  
Print["w=",w];
```

《計算結果》

```
w={ {0, 0, 0, 0}, {0, 0, 1, 0}, {0, 1, 0, 0}, {0, 1, 1, 0}, {0, 2, 0, 0}, {0, 2, 1, 0},  
    {1, 0, 0, 0}, {1, 0, 1, 0}, {1, 1, 0, 0}, {1, 1, 1, 0}, {1, 2, 0, 0}, {1, 2, 1, 0},  
    {2, 0, 0, 0}, {2, 0, 1, 0}, {2, 1, 0, 0}, {2, 1, 1, 0}, {2, 2, 0, 0}, {2, 2, 1, 0},  
    {3, 0, 0, 0}, {3, 0, 1, 0}, {3, 1, 0, 0}, {3, 1, 1, 0}, {3, 2, 0, 0}, {3, 2, 1, 0} }
```

6. $x_1, x_2, \dots, x_n$ の v による多項式表現

(4.1) より v のべき乗 $v^0, v^1, \dots, v^{n!-1}$ は $x_1, x_2, \dots, x_n$ の多項式となり、さらに第2節で述べた方法によって次数を低減させれば、基底 $w_1, w_2, \dots, w_{n!}$ の1次式で表される。これらを行列を用いて次式のように表し、その係数 a_{ij} ($1 \leq i \leq n!, 1 \leq j \leq n!$) を計算する。

$$\begin{bmatrix} v^0 \\ v^1 \\ \vdots \\ v^{n!-1} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n!} \\ a_{21} & a_{22} & \cdots & a_{2n!} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n!1} & a_{n!2} & \cdots & a_{n!n!} \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_{n!} \end{bmatrix} \quad (6.1)$$

これを $w_1, w_2, \dots, w_{n!}$ について解けば、これらが v の多項式として求められる。クラメールの方法によると、(6.1) の右辺の係数行列を A 、左辺の列ベクトルを b 、 A の第 i 列を b で置換した行列を A_i とすれば、 w_i は次式で与えられる。

$$w_i = \det(A_i) / \det(A) \quad (6.2)$$

ここで、 $\det(A_i)$ は A_i の行列式、 $\det(A)$ は A の行列式である。 x_n を除いた $x_1, x_2, \dots, x_{n-1}$ は $w_1, w_2, \dots, w_{n!}$ のどれかと一致し、前節で決めた $w_1, w_2, \dots, w_{n!}$ の順序によれば、 $x_1, x_2, \dots, x_{n-1}$ は次式となる。

$$x_1 = w_{(n-1)!+1}, x_2 = w_{(n-2)!+1}, \dots, x_{n-1} = w_{1!+1} \quad (6.3)$$

他の w_i は不要であるから、 $\det(A)$ と $n-1$ 個の $\det(A_i)$ だけを計算すれば十分である。連立1次方程式の解法として、クラメールの方法は $w_1, w_2, \dots, w_{n!}$ のすべてを求める場合は非効率的であるが、一部だけを求めればよい場合は効率的である。残りの x_n は次式となる。

$$x_n = -a_{n-1} - (x_1 + x_2 + \cdots + x_{n-1}) \quad (6.4)$$

これで $x_1, x_2, \dots, x_n$ が v の多項式として求められた。さらに、 $g(x)$ の次数が $n!$ より小さい場合は、 $x_1, x_2, \dots, x_n$ の $g(v)$ による剰余を改めて $x_1, x_2, \dots, x_n$ とすることにより、 v の次数を低減させる。

(例1) $f(x) = x^3 + a_2 x^2 + a_1 x + a_0$ の場合

$v = x_1 - x_2$ とする。 v のべき乗は次式となる。

$$v^2 = -a_1 - a_2(x_1 + x_2) - 3x_1 x_2 \quad (6.5)$$

$$v^3 = 3a_0 - a_1 a_2 + (a_1 - a_2^2)x_2 + (-a_1 - a_2^2)x_1 - 4a_2 x_1 x_2 - 2a_2 x_1^2 - 6x_1^2 x_2 \quad (6.6)$$

$$v^4 = a_1^2 + 6a_0 a_2 - a_1 a_2^2 + (9a_0 + 2a_1 a_2 - a_2^3)(x_1 + x_2) + (15a_1 - 5a_2^2)x_1 x_2 \quad (6.7)$$

$$v^5 = -6a_0 a_1 + 2a_1^2 a_2 + 5a_0 a_2^2 - a_1 a_2^3 + (-a_1^2 + 3a_0 a_2 + 3a_1 a_2^2 - a_2^4)x_2 + (a_1^2 + 15a_0 a_2 + a_1 a_2^2 - a_2^4)x_1 \\ + (9a_0 + 17a_1 a_2 - 6a_2^3)x_1 x_2 + (18a_0 + 4a_1 a_2 - 2a_2^3)x_1^2 + (30a_1 - 10a_2^2)x_1^2 x_2 \quad (6.8)$$

これより、(6.1) は次式となる。

$$\begin{bmatrix} v^0 \\ v^1 \\ v^2 \\ v^3 \\ v^4 \\ v^5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ -a_1 & -a_2 & -a_2 \\ 3a_0 - a_1 a_2 & a_1 - a_2^2 & -a_1 - a_2^2 \\ a_1^2 + 6a_0 a_2 - a_1 a_2^2 & 9a_0 + 2a_1 a_2 - a_2^3 & 9a_0 + 2a_1 a_2 - a_2^3 \\ -6a_0 a_1 + 2a_1^2 a_2 + 5a_0 a_2^2 - a_1 a_2^3 & -a_1^2 + 3a_0 a_2 + 3a_1 a_2^2 - a_2^4 & a_1^2 + 15a_0 a_2 + a_1 a_2^2 - a_2^4 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -3 & 0 & 0 \\ -4a_2 & -2a_2 & -6 \\ 15a_1 - 5a_2^2 & 0 & 0 \\ 9a_0 + 17a_1a_2 - 6a_2^3 & 18a_0 + 4a_1a_2 - 2a_2^3 & 30a_1 - 10a_2^2 \end{bmatrix} \begin{bmatrix} 1 \\ x_2 \\ x_1 \\ x_1x_2 \\ x_1^2 \\ x_1^2x_2 \end{bmatrix} \quad (6.9)$$

これより, x_1, x_2, x_3 は次式となる。

$$x_1 = \{3v^4 + 5(3a_1 - a_2^2)v^2 + (27a_0 - 9a_1a_2 + 2a_2^3)v + 2(6a_1^2 - 9a_0a_2 - a_1a_2^2)\} / 2D \quad (6.10)$$

$$x_2 = \{3v^4 + 5(3a_1 - a_2^2)v^2 - (27a_0 - 9a_1a_2 + 2a_2^3)v + 2(6a_1^2 - 9a_0a_2 - a_1a_2^2)\} / 2D \quad (6.11)$$

$$x_3 = \{-3v^4 - 5(3a_1 - a_2^2)v^2 - 12a_1^2 - 9a_0a_2 + 11a_1a_2^2 - 2a_2^4\} / D \quad (6.12)$$

$$D = 27a_0 - 9a_1a_2 + 2a_2^3 \quad (6.13)$$

(例2) $f(x) = x^4 + a_2x^2 + a_0$ の場合

第4節の(例3)より $v = x_1 + 2x_2 - 2x_3$ とする。(6.1)の右辺の係数行列は大きい(24行×24列)ので省略する。 x_1, x_2, x_3, x_4 も長い(v の23次式)ので省略する。さらに, これらの $g(v)$ ((4.8)の $g(x)$ に $x=v$ を代入したもの)による剰余を改めて x_1, x_2, x_3, x_4 とし, v の次数を低減させると次式が得られる。

$$x_1 = \{7a_2v^7 + 10(25a_0 + 3a_2^2)v^5 + a_2(1777a_0 - 69a_2^2)v^3 - (4750a_0^2 - 3945a_0a_2^2 + 308a_2^4)v\} / D \quad (6.14)$$

$$x_2 = -\{7a_2v^7 + 10(25a_0 + 3a_2^2)v^5 + a_2(1777a_0 - 69a_2^2)v^3 - (4750a_0^2 - 3945a_0a_2^2 + 308a_2^4)v\} / D \quad (6.15)$$

$$x_3 = -\{7a_2v^7 + 10(25a_0 + 3a_2^2)v^5 + a_2(1777a_0 - 69a_2^2)v^3 + (10250a_0^2 + 195a_0a_2^2 - 92a_2^4)v\} / 2D \quad (6.16)$$

$$x_4 = \{7a_2v^7 + 10(25a_0 + 3a_2^2)v^5 + a_2(1777a_0 - 69a_2^2)v^3 + (10250a_0^2 + 195a_0a_2^2 - 92a_2^4)v\} / 2D \quad (6.17)$$

$$D = 6(25a_0 - 4a_2^2)(100a_0 - 9a_2^2) \quad (6.18)$$

数式処理ソフトによる計算

《サブプログラム》

$V[1]$ のべき乗と基底 $w[1], w[2], \dots, w[n!]$ の関係を表す行列 A を計算する。

(* Calculation of Powers of $V[1]$ *)

```
PowerOfV[]:=Module[{Ai, c, i, j, k},
  A={};
  AppendTo[A, Table[If[j==1, 1, 0], {j, 1, nn}]];
  c[0]=1;
  For[i=2, i<=nn, i++,
    Ai={};
    c[0]=ReductionOfX[V[1]*c[0]];
    For[j=1, j<=nn, j++,
      For[k=1, k<=n-1, k++,
        If[j!=1, If[Part[w, j, k]==Part[w, j-1, k], Continue[]]];
        c[k]=Coefficient[c[k-1], X[k], Part[w, j, k]]
      ];
      AppendTo[Ai, c[n-1]]
    ];
    AppendTo[A, Ai]
  ]
];
```

ここで

Coefficient[f, x, n] : 多項式fについて, xのn次の項の係数を求める。

《サブプログラム(2)》

クラメル方法により, 根X[1], X[2], ..., X[n]をvの多項式として求める。

```
(* X[1], X[2], ..., X[n] as Polynomials of v *)
XOfV[]:=Module[{b, bi, delta, i},
  A=Transpose[A];
  b=Table[v^i, {i, 0, nn-1}];
  If[n>=5, Print["..... calculating (1/", n, ") ....."]];
  delta=Det[A];
  For[i=1, i<=n-1, i++,
    If[n>=5, Print["..... calculating (", i+1, "/", n, ") ....."]];
    bi=Part[A, Factorial[n-i]+1];
    Part[A, Factorial[n-i]+1]=b;
    X[i]=Simplify[Det[A]/delta];
    Part[A, Factorial[n-i]+1]=bi
  ];
  X[n]=-Coefficient[fx, x, n-1]-Sum[X[i], {i, 1, n-1}];
  For[i=1, i<=n, i++,
    X[i]=Simplify[PolynomialRemainder[X[i], ReplaceAll[fx, x->v], v]]
  ];
  For[i=1, i<=nn, i++,
    V[i]=Simplify[V[i]]
  ];
  Remove[A]
];
```

ここで

Transpose[A] : 行列Aの転置行列を求める。

If[n>=5, Print[...]] : $n \geq 5$ では計算時間が長くなるため, 経過を表示する。

Det[A] : 行列Aの行列式を求める。

Part[A, Factorial[n-i]+1] : 行列Aの $(n-i)!+1$ 番目の行を表す。

ReplaceAll[f, rules] : 数式fに規則rulesを適用する。x->vはxにvを代入する。

Remove[a, b, ...] : 変数a, b, ...を削除する。

《メインプログラム》

```

fx=x^4+a2*x^2+a0;
n=Exponent[fx,x];
nn=Factorial[n];
RelationsOfX[fx];
sigma=Permutations[Table[i,{i,1,n}]];
PrimitiveElement[];
MinimalPolynomial[];
BasisOfSplittingField[];
PowerOfV[];
XOfV[];
For[i=1,i<=n,i++,
  Print["X[" , i, "]=",X[i]]
];

```

《計算結果》

```

m[1]=1
m[2]=2
m[3]=-2
m[4]=0

```

factors of $g(x)$:

- (1) $625a^2 - 200a^0 a^2 + 16a^4 - 70a^0 a^2 x^2 + 40a^2 x^2 - 14a^0 x^4 + 33a^2 x^4 + 10a^2 x^6 + x^8$
- (2) $28561a^2 - 12168a^0 a^2 + 1296a^4 - 3094a^0 a^2 x^2 + 936a^2 x^2 - 238a^0 x^4 + 241a^2 x^4 + 26a^2 x^6 + x^8$
- (3) $83521a^2 - 9248a^0 a^2 + 256a^4 + 5474a^0 a^2 x^2 + 544a^2 x^2 + 322a^0 x^4 + 321a^2 x^4 + 34a^2 x^6 + x^8$

入力要求"Select one of factors : "に対して"1"を入力する(1番目の因数を選ぶ)と

```

X[1]=(v(-4750a0^2+a0(3945a2^2+1777a2 v^2+250v^4)+a2(-308a2^3-69a2^2v^2+30a2 v^4+7v^6)))/
(6(100a0-9a2^2)(25a0-4a2^2))
X[2]=- (v(-4750a0^2+a0(3945a2^2+1777a2 v^2+250v^4)+a2(-308a2^3-69a2^2v^2+30a2 v^4+7v^6)))/
(6(2500a0^2-625a0 a2^2+36a2^4))
X[3]=- (v(10250a0^2+a0(195a2^2+1777a2 v^2+250v^4)+a2(-92a2^3-69a2^2v^2+30a2 v^4+7v^6)))/
(12(2500a0^2-625a0 a2^2+36a2^4))
X[4]=(v(10250a0^2+a0(195a2^2+1777a2 v^2+250v^4)+a2(-92a2^3-69a2^2v^2+30a2 v^4+7v^6)))/
(12(2500a0^2-625a0 a2^2+36a2^4))

```

7. ガロア群Gの計算法

第4節より $g(x)$ の根は $v_1, v_2, \dots, v_n$ またはその一部である。 $v_1, v_2, \dots, v_n$ の中で $g(x)$ の根であるものを v_i とし、これに対応する置換 σ_i を集めて、これをガロア群 G とする。 v_i が $g(x)$ の根であるかどうかは、以下のようにして調べる。まず、 $x_1, x_2, \dots, x_n$ は v の多項式で表されるので、(4.1)より v_i も v の多項式で表される。これを $g(x)$ に代入して、 $g(v)$ による剰余が0であれば、 v_i は $g(x)$ の根である。

(例1) $f(x)=x^3+a_2x^2+a_1x+a_0$ の場合

(4.3)より $g(x)$ の次数は6であるから、すべての置換がガロア群 G に含まれる。

$$G=\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\} \quad (7.1)$$

x_1, x_2, x_3 を $x_{j_1}, x_{j_2}, x_{j_3}$ に移す置換を $\{j_1, j_2, j_3\}$ で表すと以下ようになる。

$$G=\{\{1, 2, 3\}, \{1, 3, 2\}, \{2, 1, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{3, 2, 1\}\} \quad (7.2)$$

(例2) $f(x)=x^4+a_2x^2+a_0$ の場合

$v=x_1+2x_2-2x_3$ と(6.14)–(6.18)より、 v_i と $g(v_i)$ ($i=1, 2, \dots, 24$)は次式となる。

$$\begin{aligned} v_1 &= -v_8 = v \\ g(v_1) &= g(v_8) = 0 \end{aligned} \quad (7.3)$$

$$\begin{aligned} v_2 &= -v_7 = \{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3+10(275a_0^2+207a_0a_2^2-20a_2^4)v\}/3D_1D_2 \\ g(v_2) &= g(v_7) = 0 \end{aligned} \quad (7.4)$$

$$\begin{aligned} v_3 &= -v_{11} = \{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3-2(6125a_0^2-2910a_0a_2^2+208a_2^4)v\}/3D_1D_2 \\ g(v_3) &= g(v_{11}) = \{16a_2(5116a_0+785a_2^2)v^6-240(1400a_0^2-2034a_0a_2^2-451a_2^4)v^4 \\ &\quad -16a_2(104524a_0^2-6499a_0a_2^2-16440a_2^4)v^2+32(25a_0-4a_2^2)(2460a_0^2+5713a_0a_2^2-970a_2^4)\}/3D_2 \end{aligned} \quad (7.5)$$

$$\begin{aligned} v_4 &= -v_{12} = \{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3+(25250a_0^2-3555a_0a_2^2+124a_2^4)v\}/6D_1D_2 \\ g(v_4) &= g(v_{12}) = \{48a_2(1036a_0+45a_2^2)v^6+240(1400a_0^2+78a_0a_2^2+189a_2^4)v^4 \\ &\quad -48a_2(15404a_0^2-1839a_0a_2^2-1755a_2^4)v^2+48(11000a_0^3+29850a_0^2a_2^2-10394a_0a_2^4+855a_2^6)\}/D_2 \end{aligned} \quad (7.6)$$

$$\begin{aligned} v_5 &= -v_9 = \{14a_2v^7+20(25a_0+3a_2^2)v^5+2a_2(1777a_0-69a_2^2)v^3-(2000a_0^2-6015a_0a_2^2+508a_2^4)v\}/3D_1D_2 \\ g(v_5) &= g(v_9) = \{112a_2(412a_0-55a_2^2)v^6+240(1400a_0^2+1966a_0a_2^2-251a_2^4)v^4+16a_2(192524a_0^2 \\ &\quad +93901a_0a_2^2-11640a_2^4)v^2-32(85500a_0^3-270775a_0^2a_2^2-36358a_0a_2^4+5480a_2^6)\}/3D_2 \end{aligned} \quad (7.7)$$

$$\begin{aligned} v_6 &= -v_{10} = \{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3+(5250a_0^2+1445a_0a_2^2-164a_2^4)v\}/2D_1D_2 \\ g(v_6) &= g(v_{10}) = \{48a_2(1436a_0-855a_2^2)v^6+240(1400a_0^2+678a_0a_2^2-1161a_2^4)v^4-144a_2(3668a_0^2 \\ &\quad +1087a_0a_2^2+3015a_2^4)v^2-48(109000a_0^3+111550a_0^2a_2^2-46544a_0a_2^4+4095a_2^6)\}/D_2 \end{aligned} \quad (7.8)$$

$$\begin{aligned} v_{13} &= -v_{21} = \{49a_2v^7+70(25a_0+3a_2^2)v^5+7a_2(1777a_0-69a_2^2)v^3-(48250a_0^2-31365a_0a_2^2+2372a_2^4)v\}/12D_1D_2 \\ g(v_{13}) &= g(v_{21}) = \{48a_2(1436a_0-855a_2^2)v^6-480(700a_0^2-1815a_0a_2^2+702a_2^4)v^4-336a_2(11572a_0^2 \\ &\quad -10077a_0a_2^2+2160a_2^4)v^2+48(109000a_0^3-118470a_0^2a_2^2+31901a_0a_2^4-2880a_2^6)\}/D_2 \end{aligned} \quad (7.9)$$

$$\begin{aligned} v_{14} &= -v_{22} = \{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3-(49750a_0^2-15195a_0a_2^2+956a_2^4)v\}/12D_1D_2 \\ g(v_{14}) &= g(v_{22}) = \{-112a_2(412a_0-55a_2^2)v^6+480(700a_0^2-459a_0a_2^2+67a_2^4)v^4+16a_2(17476a_0^2 \\ &\quad -15301a_0a_2^2+2865a_2^4)v^2-16(171000a_0^3-103930a_0^2a_2^2+20039a_0a_2^4-1240a_2^6)\}/3D_2 \end{aligned} \quad (7.10)$$

$$\begin{aligned} v_{15} &= -v_{19} = \{21a_2v^7+30(25a_0+3a_2^2)v^5+3a_2(1777a_0-69a_2^2)v^3-(9250a_0^2-10585a_0a_2^2+852a_2^4)v\}/4D_1D_2 \\ g(v_{15}) &= g(v_{19}) = \{48a_2(1036a_0+45a_2^2)v^6-480(700a_0^2-1515a_0a_2^2+27a_2^4)v^4-144a_2(28468a_0^2 \\ &\quad -25213a_0a_2^2+1440a_2^4)v^2-48(11000a_0^3+281870a_0^2a_2^2-139339a_0a_2^4+10080a_2^6)\}/D_2 \end{aligned} \quad (7.11)$$

$$\begin{aligned} v_{16} &= -v_{20} = \{49a_2v^7+70(25a_0+3a_2^2)v^5+7a_2(1777a_0-69a_2^2)v^3+(11750a_0^2+16365a_0a_2^2-1508a_2^4)v\}/12D_1D_2 \\ g(v_{16}) &= g(v_{20}) = \{16a_2(5116a_0+785a_2^2)v^6+480(700a_0^2+1541a_0a_2^2+167a_2^4)v^4 \\ &\quad +112a_2(15068a_0^2+12157a_0a_2^2+1095a_2^4)v^2-16(20a_0+43a_2^2)(6150a_0^2-43a_0a_2^2-80a_2^4)\}/3D_2 \end{aligned} \quad (7.12)$$

$$\begin{aligned} v_{17} &= -v_{24} = \{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3-5(1950a_0^2-1039a_0a_2^2+76a_2^4)v\}/4D_1D_2 \\ g(v_{17}) &= g(v_{24}) = 0 \end{aligned} \quad (7.13)$$

$$v_{18} = -v_{23} = \{35a_2v^7+50(25a_0+3a_2^2)v^5+5a_2(1777a_0-69a_2^2)v^3-(8750a_0^2-15975a_0a_2^2+1324a_2^4)v\}/12D_1D_2$$

$$g(v_{18})=g(v_{23})=0 \quad (7.14)$$

ここで

$$D_1=25a_0-4a_2^2, \quad D_2=100a_0-9a_2^2 \quad (7.15)$$

これより, $g(x)$ の根は $v_1, v_2, v_7, v_8, v_{17}, v_{18}, v_{23}, v_{24}$ である。ガロア群 G は以下のようにになる。

$$G=\{\sigma_1, \sigma_2, \sigma_7, \sigma_8, \sigma_{17}, \sigma_{18}, \sigma_{23}, \sigma_{24}\} \quad (7.16)$$

x_1, x_2, x_3, x_4 を $x_{j_1}, x_{j_2}, x_{j_3}, x_{j_4}$ に移す置換を $\{j_1, j_2, j_3, j_4\}$ で表すと以下のようにになる。

$$G=\{\{1, 2, 3, 4\}, \{1, 2, 4, 3\}, \{2, 1, 3, 4\}, \{2, 1, 4, 3\}, \{3, 4, 1, 2\}, \{3, 4, 2, 1\}, \\ \{4, 3, 1, 2\}, \{4, 3, 2, 1\}\} \quad (7.17)$$

数式処理ソフトによる計算

《サブプログラム》

ガロア群 G を求める。

```
(* Calculation of Galois Group *)
GaloisGroup[]:=Module[{gv, i, j},
  If[Exponent[ gx, x]==nn, G=sigma; Return[]];
  G={};
  For[i=1, i<=nn, i++,
    gv=0;
    For[j=Exponent[ gx, x], j>=0, j--,
      gv=Simplify[PolynomialRemainder[
        gv*V[i]+Coefficient[ gx, x, j], ReplaceAll[ gx, x->v], v]]
    ];
    If[Exponent[ gv, v]<0, AppendTo[G, i]]
  ];
  nn=Length[G];
  For[i=1, i<=nn, i++,
    V[i]=V[Part[G, i]];
    Part[G, i]=Part[sigma, Part[G, i]]
  ]
];
```

《メインプログラム》

```
fx=x^4+a2*x^2+a0;
n=Exponent[fx, x];
nn=Factorial[n];
RelationsOfX[fx];
sigma=Permutations[Table[i, {i, 1, n}]];
PrimitiveElement[];
MinimalPolynomial[];
BasisOfSplittingField[];
PowerOfV[];
XOfV[];
GaloisGroup[];
Print["G=", G];
```


《計算結果》

$$m[1]=1$$

$$m[2]=2$$

$$m[3]=-2$$

$$m[4]=0$$

factors of $g(x)$:

$$(1) 625a^0 - 200a^0 a^2 + 16a^2 - 70a^0 a^2 x^2 + 40a^2 x^2 - 14a^0 x^4 + 33a^2 x^4 + 10a^2 x^6 + x^8$$

$$(2) 28561a^0 - 12168a^0 a^2 + 1296a^2 - 3094a^0 a^2 x^2 + 936a^2 x^2 - 238a^0 x^4 + 241a^2 x^4 + 26a^2 x^6 + x^8$$

$$(3) 83521a^0 - 9248a^0 a^2 + 256a^2 + 5474a^0 a^2 x^2 + 544a^2 x^2 + 322a^0 x^4 + 321a^2 x^4 + 34a^2 x^6 + x^8$$

入力要求”Select one of factors : ”に対して”1”を入力する(1番目の因数を選ぶ) と

$$G = \{ \{1, 2, 3, 4\}, \{1, 2, 4, 3\}, \{2, 1, 3, 4\}, \{2, 1, 4, 3\}, \{3, 4, 1, 2\}, \{3, 4, 2, 1\},$$

$$\{4, 3, 1, 2\}, \{4, 3, 2, 1\} \}$$

8. ガロア群 G の乗積表と逆元

ガロア群 G は置換 $\sigma_1, \sigma_2, \dots, \sigma_n$ の部分群である。 G に属する元の個数を N とし、これらの元に改めて番号を付け直して $\sigma_1, \sigma_2, \dots, \sigma_N$ とする。これに対して、以下のようにして、乗積表と逆元を求める。
 $\sigma_i = \{i_1, i_2, \dots, i_n\}$ と $\sigma_j = \{j_1, j_2, \dots, j_n\}$ の積 $\sigma_i \sigma_j$ は次式で与えられる。

$$\sigma_i \sigma_j = \{i_{j_1}, i_{j_2}, \dots, i_{j_n}\} \quad (8.1)$$

$\sigma_i = \{i_1, i_2, \dots, i_n\}$ の逆元を $\sigma_i^{-1} = \{j_1, j_2, \dots, j_n\}$ とすると、 $j_k (k=1, 2, \dots, n)$ は次式で与えられる。

$$\begin{aligned} j_k &= 1 \quad (i_1 = k \text{ の場合}) \\ &= 2 \quad (i_2 = k \text{ の場合}) \\ &\dots \dots \dots \\ &= n \quad (i_n = k \text{ の場合}) \end{aligned} \quad (8.2)$$

(例) $n=4, N=24$ の場合

以下に積 $\sigma_i \sigma_j$ の乗積表を示す。例えば、 $\sigma_8 = \{2, 1, 4, 3\}$ と $\sigma_{17} = \{3, 4, 1, 2\}$ の積は $\sigma_{24} = \{4, 3, 2, 1\}$ である。

$i \setminus j$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	2	1	5	6	3	4	8	7	11	12	9	10	19	20	21	22	23	24	13	14	15	16	17	18
3	3	4	1	2	6	5	13	14	15	16	17	18	7	8	9	10	11	12	20	19	23	24	21	22
4	4	3	6	5	1	2	14	13	17	18	15	16	20	19	23	24	21	22	7	8	9	10	11	12
5	5	6	2	1	4	3	19	20	21	22	23	24	8	7	11	12	9	10	14	13	17	18	15	16
6	6	5	4	3	2	1	20	19	23	24	21	22	14	13	17	18	15	16	8	7	11	12	9	10
7	7	8	9	10	11	12	1	2	3	4	5	6	15	16	13	14	18	17	21	22	19	20	24	23
8	8	7	11	12	9	10	2	1	5	6	3	4	21	22	19	20	24	23	15	16	13	14	18	17
9	9	10	7	8	12	11	15	16	13	14	18	17	1	2	3	4	5	6	22	21	24	23	19	20
10	10	9	12	11	7	8	16	15	18	17	13	14	22	21	24	23	19	20	1	2	3	4	5	6
11	11	12	8	7	10	9	21	22	19	20	24	23	2	1	5	6	3	4	16	15	18	17	13	14
12	12	11	10	9	8	7	22	21	24	23	19	20	16	15	18	17	13	14	2	1	5	6	3	4
13	13	14	15	16	17	18	3	4	1	2	6	5	9	10	7	8	12	11	23	24	20	19	22	21
14	14	13	17	18	15	16	4	3	6	5	1	2	23	24	20	19	22	21	9	10	7	8	12	11
15	15	16	13	14	18	17	9	10	7	8	12	11	3	4	1	2	6	5	24	23	22	21	20	19
16	16	15	18	17	13	14	10	9	12	11	7	8	24	23	22	21	20	19	3	4	1	2	6	5
17	17	18	14	13	16	15	23	24	20	19	22	21	4	3	6	5	1	2	10	9	12	11	7	8
18	18	17	16	15	14	13	24	23	22	21	20	19	10	9	12	11	7	8	4	3	6	5	1	2
19	19	20	21	22	23	24	5	6	2	1	4	3	11	12	8	7	10	9	17	18	14	13	16	15
20	20	19	23	24	21	22	6	5	4	3	2	1	17	18	14	13	16	15	11	12	8	7	10	9
21	21	22	19	20	24	23	11	12	8	7	10	9	5	6	2	1	4	3	18	17	16	15	14	13
22	22	21	24	23	19	20	12	11	10	9	8	7	18	17	16	15	14	13	5	6	2	1	4	3
23	23	24	20	19	22	21	17	18	14	13	16	15	6	5	4	3	2	1	12	11	10	9	8	7
24	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

以下に σ_i の逆元 σ_j を示す。例えば、 $\sigma_{10}=\{2, 3, 4, 1\}$ の逆元は $\sigma_{19}=\{4, 1, 2, 3\}$ である。

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
j	1	2	3	5	4	6	7	8	13	19	14	20	9	11	15	21	17	23	10	12	16	22	18	24

数式処理ソフトによる計算

《サブプログラム》

ガロア群Gの乗積表ListOfProductを求める。

```
(* Products of Galois Group *)
ProductOfG[]:=Module[{i, j, k, p, temp},
  ListOfProduct={};
  For[i=1, i<=nn, i++,
    temp={};
    For[j=1, j<=nn, j++,
      p=Table[Part[G, i, Part[G, j, k]], {k, 1, n}];
      AppendTo[temp, Part[Position[G, p], 1, 1]]
    ];
    AppendTo[ListOfProduct, temp]
  ]
];
```

ここで

Part[Position[v, x], 1, 1] : 配列v中の要素xの位置を求める。

《サブプログラム(2)》

ガロア群Gの逆元ListOfInverseを求める。

```
(* Inverses of Galois Group *)
InverseOfG[]:=Module[{i, j, k, p},
  ListOfInverse={};
  For[i=1, i<=nn, i++,
    For[k=1, k<=n, k++, j[Part[G, i, k]]=k];
    p=Table[j[k], {k, 1, n}];
    AppendTo[ListOfInverse, Part[Position[G, p], 1, 1]]
  ]
];
```

《メインプログラム》

```
n=4;
nn=Factorial[n];
G=Permutations[Table[i, {i, 1, n}]];
ProductOfG[];
Print["product of G : "];
Print[ListOfProduct];
InverseOfG[];
Print["inverse of G : "];
Print[ListOfInverse];
```

《計算結果》

```
product of G :
{{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24},
 {2, 1, 5, 6, 3, 4, 8, 7, 11, 12, 9, 10, 19, 20, 21, 22, 23, 24, 13, 14, 15, 16, 17, 18},
 {3, 4, 1, 2, 6, 5, 13, 14, 15, 16, 17, 18, 7, 8, 9, 10, 11, 12, 20, 19, 23, 24, 21, 22},
 {4, 3, 6, 5, 1, 2, 14, 13, 17, 18, 15, 16, 20, 19, 23, 24, 21, 22, 7, 8, 9, 10, 11, 12},
 {5, 6, 2, 1, 4, 3, 19, 20, 21, 22, 23, 24, 8, 7, 11, 12, 9, 10, 14, 13, 17, 18, 15, 16},
 {6, 5, 4, 3, 2, 1, 20, 19, 23, 24, 21, 22, 14, 13, 17, 18, 15, 16, 8, 7, 11, 12, 9, 10},
 {7, 8, 9, 10, 11, 12, 1, 2, 3, 4, 5, 6, 15, 16, 13, 14, 18, 17, 21, 22, 19, 20, 24, 23},
 {8, 7, 11, 12, 9, 10, 2, 1, 5, 6, 3, 4, 21, 22, 19, 20, 24, 23, 15, 16, 13, 14, 18, 17},
 {9, 10, 7, 8, 12, 11, 15, 16, 13, 14, 18, 17, 1, 2, 3, 4, 5, 6, 22, 21, 24, 23, 19, 20},
 {10, 9, 12, 11, 7, 8, 16, 15, 18, 17, 13, 14, 22, 21, 24, 23, 19, 20, 1, 2, 3, 4, 5, 6},
 {11, 12, 8, 7, 10, 9, 21, 22, 19, 20, 24, 23, 2, 1, 5, 6, 3, 4, 16, 15, 18, 17, 13, 14},
 {12, 11, 10, 9, 8, 7, 22, 21, 24, 23, 19, 20, 16, 15, 18, 17, 13, 14, 2, 1, 5, 6, 3, 4},
 {13, 14, 15, 16, 17, 18, 3, 4, 1, 2, 6, 5, 9, 10, 7, 8, 12, 11, 23, 24, 20, 19, 22, 21},
 {14, 13, 17, 18, 15, 16, 4, 3, 6, 5, 1, 2, 23, 24, 20, 19, 22, 21, 9, 10, 7, 8, 12, 11},
 {15, 16, 13, 14, 18, 17, 9, 10, 7, 8, 12, 11, 3, 4, 1, 2, 6, 5, 24, 23, 22, 21, 20, 19},
 {16, 15, 18, 17, 13, 14, 10, 9, 12, 11, 7, 8, 24, 23, 22, 21, 20, 19, 3, 4, 1, 2, 6, 5},
 {17, 18, 14, 13, 16, 15, 23, 24, 20, 19, 22, 21, 4, 3, 6, 5, 1, 2, 10, 9, 12, 11, 7, 8},
 {18, 17, 16, 15, 14, 13, 24, 23, 22, 21, 20, 19, 10, 9, 12, 11, 7, 8, 4, 3, 6, 5, 1, 2},
 {19, 20, 21, 22, 23, 24, 5, 6, 2, 1, 4, 3, 11, 12, 8, 7, 10, 9, 17, 18, 14, 13, 16, 15},
 {20, 19, 23, 24, 21, 22, 6, 5, 4, 3, 2, 1, 17, 18, 14, 13, 16, 15, 11, 12, 8, 7, 10, 9},
 {21, 22, 19, 20, 24, 23, 11, 12, 8, 7, 10, 9, 5, 6, 2, 1, 4, 3, 18, 17, 16, 15, 14, 13},
 {22, 21, 24, 23, 19, 20, 12, 11, 10, 9, 8, 7, 18, 17, 16, 15, 14, 13, 5, 6, 2, 1, 4, 3},
 {23, 24, 20, 19, 22, 21, 17, 18, 14, 13, 16, 15, 6, 5, 4, 3, 2, 1, 12, 11, 10, 9, 8, 7},
 {24, 23, 22, 21, 20, 19, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1}}
```

```
inverse of G :
{1, 2, 3, 5, 4, 6, 7, 8, 13, 19, 14, 20, 9, 11, 15, 21, 17, 23, 10, 12, 16, 22, 18, 24}
```

9. ガロア群 G の組成列

ガロア群 G について、以下の組成列を求める。

$$G = G_0 \supset G_1 \supset \cdots \supset G_s \quad (9.1)$$

ここで、 $G_k (k=1, 2, \dots, s)$ は G_{k-1} の真部分群で最大の正規部分群とする。最後の G_s は単位群である。 k 番目の組成列 $G_{k-1} \supset G_k$ において、 G_{k-1} から G_k を求める方法を示す。まず、以下の手順により、 G_{k-1} のすべての正規部分群を求める。

- (1) G_{k-1} 中の1個の元から生成される正規部分群を求める。これには、 G_{k-1} 中の1個の元を τ 、 $S = \{\sigma^{-1}\tau\sigma \mid \sigma \in G_{k-1}\}$ とし、 S から生成される群を $\langle S \rangle$ とすれば、これが求める正規部分群となる。このようにして、1個の元から生成される正規部分群をすべて求め、これらの中から相異なるものだけを取り出す。
- (2) G_{k-1} 中の2個の元から生成される正規部分群を求める。これには、1個の元から生成される正規部分群のうちの1つを H_i 、もう1つを H_j とし、両者から生成される群を $\langle H_i, H_j \rangle$ とすれば、これが求める正規部分群となる。このようにして、2個の元から生成される正規部分群をすべて求め、これらの中から新規で相異なるものだけを取り出す。
- (3) $l=3, 4, 5, \dots$ として、 G_{k-1} 中の l 個の元から生成される正規部分群を求める。これには、 $l-1$ 個の元から生成される正規部分群のうちの1つを H_i 、1個の元から生成される正規部分群のうちの1つを H_j とし、両者から生成される群を $\langle H_i, H_j \rangle$ とすれば、これが求める正規部分群となる。このようにして、 l 個の元から生成される正規部分群をすべて求め、これらの中から新規で相異なるものだけを取り出す。ここで、 l 個の元から生成される新規の正規部分群が1つもなければ終了とする。

ここで、手順(1)において、 $\langle S \rangle$ は G_{k-1} の正規部分群となることを証明する。 $\langle S \rangle$ の元を ρ とすると、 ρ は S の元の有限個(l 個とする)の積として、次式のように表される。

$$\rho = (\sigma_1^{-1}\tau\sigma_1)(\sigma_2^{-1}\tau\sigma_2)\cdots(\sigma_l^{-1}\tau\sigma_l) \quad (\sigma_1, \sigma_2, \dots, \sigma_l \in G_{k-1}) \quad (9.2)$$

このとき、任意の $\sigma_0 \in G_{k-1}$ に対して、 $\sigma_0^{-1}\rho\sigma_0$ も S の元の有限個(m 個とする)の積として、次式のように表されることを示せばよい。

$$\begin{aligned} \sigma_0^{-1}\rho\sigma_0 &= \sigma_0^{-1}(\sigma_1^{-1}\tau\sigma_1)(\sigma_2^{-1}\tau\sigma_2)\cdots(\sigma_l^{-1}\tau\sigma_l)\sigma_0 \\ &= (\sigma_1'^{-1}\tau\sigma_1')(\sigma_2'^{-1}\tau\sigma_2')\cdots(\sigma_m'^{-1}\tau\sigma_m') \quad (\sigma_1', \sigma_2', \dots, \sigma_m' \in G_{k-1}) \end{aligned} \quad (9.3)$$

実際に $\sigma_0^{-1}\rho\sigma_0$ を上式の第2行のように表すことは可能で、例えば $l=m$ とし、 $\sigma_1', \sigma_2', \dots, \sigma_m'$ を次式のようになすればよい。

$$\sigma_1' = \sigma_1\sigma_0, \quad \sigma_2' = \sigma_2\sigma_0, \quad \dots, \quad \sigma_l' = \sigma_l\sigma_0 \quad (9.4)$$

よって、 $\langle S \rangle$ は G_{k-1} の正規部分群となる。 (証明終わり)

同様に、手順(2), (3)において、 $\langle H_i, H_j \rangle$ は G_{k-1} の正規部分群となることも証明できる。

このようにして、 G_{k-1} のすべての正規部分群が求められる。これらの正規部分群のうち、元の個数が G_{k-1} より小さく、かつ最大であるものを G_k とする。これを $k=1$ から始めて、 $k=s$ で G_s が単位群になれば終了とする。このとき、 $|G_{k-1}/G_k| (k=1, 2, \dots, s)$ がすべて素数ならば、 G は可解である。

(例1) $n=4$, $N=24$ の場合

以下の G について組成列を求める。

$$\begin{aligned} G &= \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}, \sigma_{17}, \sigma_{18}, \sigma_{19}, \sigma_{20}, \sigma_{21}, \sigma_{22}, \sigma_{23}, \sigma_{24}\} \\ &= \{\{1, 2, 3, 4\}, \{1, 2, 4, 3\}, \{1, 3, 2, 4\}, \{1, 3, 4, 2\}, \{1, 4, 2, 3\}, \{1, 4, 3, 2\}, \\ &\quad \{2, 1, 3, 4\}, \{2, 1, 4, 3\}, \{2, 3, 1, 4\}, \{2, 3, 4, 1\}, \{2, 4, 1, 3\}, \{2, 4, 3, 1\}, \\ &\quad \{3, 1, 2, 4\}, \{3, 1, 4, 2\}, \{3, 2, 1, 4\}, \{3, 2, 4, 1\}, \{3, 4, 1, 2\}, \{3, 4, 2, 1\}, \\ &\quad \{4, 1, 2, 3\}, \{4, 1, 3, 2\}, \{4, 2, 1, 3\}, \{4, 2, 3, 1\}, \{4, 3, 1, 2\}, \{4, 3, 2, 1\}\} \end{aligned} \quad (9.5)$$

$G=G_0$ の正規部分群は以下の4個である。

$$\begin{aligned} &\{\sigma_1\} \\ &\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}, \sigma_{17}, \sigma_{18}, \sigma_{19}, \sigma_{20}, \sigma_{21}, \sigma_{22}, \sigma_{23}, \sigma_{24}\} \\ &\{\sigma_1, \sigma_4, \sigma_5, \sigma_8, \sigma_9, \sigma_{12}, \sigma_{13}, \sigma_{16}, \sigma_{17}, \sigma_{20}, \sigma_{21}, \sigma_{24}\}, \quad \{\sigma_1, \sigma_8, \sigma_{17}, \sigma_{24}\} \end{aligned}$$

これより、以下を G_1 とする。

$$G_1 = \{\sigma_1, \sigma_4, \sigma_5, \sigma_8, \sigma_9, \sigma_{12}, \sigma_{13}, \sigma_{16}, \sigma_{17}, \sigma_{20}, \sigma_{21}, \sigma_{24}\} \quad (9.6)$$

G_1 の正規部分群は以下の3個である。

$$\{\sigma_1\}, \quad \{\sigma_1, \sigma_4, \sigma_5, \sigma_8, \sigma_9, \sigma_{12}, \sigma_{13}, \sigma_{16}, \sigma_{17}, \sigma_{20}, \sigma_{21}, \sigma_{24}\}, \quad \{\sigma_1, \sigma_8, \sigma_{17}, \sigma_{24}\}$$

これより、以下を G_2 とする。

$$G_2 = \{\sigma_1, \sigma_8, \sigma_{17}, \sigma_{24}\} \quad (9.7)$$

G_2 の正規部分群は以下の5個である。

$$\{\sigma_1\}, \quad \{\sigma_1, \sigma_8\}, \quad \{\sigma_1, \sigma_{17}\}, \quad \{\sigma_1, \sigma_{24}\}, \quad \{\sigma_1, \sigma_8, \sigma_{17}, \sigma_{24}\}$$

これより、以下を G_3 とする。

$$G_3 = \{\sigma_1, \sigma_8\} \quad (9.8)$$

G_3 の正規部分群は以下の2個である。

$$\{\sigma_1\}, \quad \{\sigma_1, \sigma_8\}$$

これより、以下を G_4 とする。

$$G_4 = \{\sigma_1\} \quad (9.9)$$

$|G_0/G_1|=2$, $|G_1/G_2|=3$, $|G_2/G_3|=2$, $|G_3/G_4|=2$ はすべて素数であるから、 G は可解群である。

(例2) $n=6$, $N=8$ の場合

以下の G について組成列を求める。

$$\begin{aligned} G &= \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8\} \\ &= \{\{1, 2, 3, 4, 5, 6\}, \{1, 2, 3, 4, 6, 5\}, \{1, 2, 4, 3, 5, 6\}, \{1, 2, 4, 3, 6, 5\}, \\ &\quad \{2, 1, 3, 4, 5, 6\}, \{2, 1, 3, 4, 6, 5\}, \{2, 1, 4, 3, 5, 6\}, \{2, 1, 4, 3, 6, 5\}\} \end{aligned} \quad (9.10)$$

$G=G_0$ の正規部分群は以下の16個である。

$$\begin{aligned} &\{\sigma_1\}, \quad \{\sigma_1, \sigma_2\}, \quad \{\sigma_1, \sigma_3\}, \quad \{\sigma_1, \sigma_4\}, \quad \{\sigma_1, \sigma_5\}, \quad \{\sigma_1, \sigma_6\}, \quad \{\sigma_1, \sigma_7\}, \quad \{\sigma_1, \sigma_8\} \\ &\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}, \quad \{\sigma_1, \sigma_2, \sigma_5, \sigma_6\}, \quad \{\sigma_1, \sigma_2, \sigma_7, \sigma_8\}, \quad \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\} \\ &\{\sigma_1, \sigma_3, \sigma_6, \sigma_8\}, \quad \{\sigma_1, \sigma_4, \sigma_5, \sigma_8\}, \quad \{\sigma_1, \sigma_4, \sigma_6, \sigma_7\}, \quad \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8\} \end{aligned}$$

これより、以下を G_1 とする。

$$G_1 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\} \quad (9.11)$$

G_1 の正規部分群は以下の5個である。

$$\{\sigma_1\}, \quad \{\sigma_1, \sigma_2\}, \quad \{\sigma_1, \sigma_3\}, \quad \{\sigma_1, \sigma_4\}, \quad \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

これより、以下を G_2 とする。

$$G_2 = \{\sigma_1, \sigma_2\} \quad (9.12)$$

G_2 の正規部分群は以下の2個である。

$$\{\sigma_1\}, \quad \{\sigma_1, \sigma_2\}$$

これより，以下を G_3 とする。

$$G_3 = \{\sigma_1\}$$

(9.13)

$|G_0/G_1|=2$, $|G_1/G_2|=2$, $|G_2/G_3|=2$ はすべて素数であるから， G は可解群である。

数式処理ソフトによる計算

《サブプログラム》

H_i, H_j から生成される部分群 H を求める。

```
(* Subgroup H=<Hi, Hj> *)
Subgroup[Hi_, Hj_]:=Module[{H, i, j, k, L, p},
  H=Hi;
  For[i=1, i<=Length[Hj], i++,
    If[!MemberQ[H, Part[Hj, i]], AppendTo[H, Part[Hj, i]]]
  ];
  k=Length[Hi];
  L=Length[H];
  While[k<L,
    For[i=1, i<=L, i++,
      For[j=1, j<=L, j++,
        If[i<=k && j<=k, Continue[]];
        p=Part[ListOfProduct, Part[H, i], Part[H, j]];
        If[!MemberQ[H, p], AppendTo[H, p]]
      ]
    ];
    k=L;
    L=Length[H]
  ];
  Return[Sort[H]]
];
```

ここで

Continue[] : For, Whileなどにおいて，後の手続きは実行せず，末尾まで飛び越す。

MemberQ[v, x] : 配列v中にxがあれば真，なければ偽とする。

Sort[v] : 配列v中の要素を小さい順に並べ替える。

《サブプログラム(2)》

すべての正規部分群を求める。

```
(* Calculation of All Normal Subgroups *)
AllNormalSubgroups[G_] := Module[{Hi, Hij, Hj, i, j, k, p, S, t},
  H = {};
  For[i = 1, i <= Length[G], i++,
    S = {};
    For[j = 1, j <= Length[G], j++,
      p = Part[ListOfProduct, Part[ListOfInverse, Part[G, j]],
        Part[ListOfProduct, Part[G, i], Part[G, j]]];
      If[!MemberQ[S, p], AppendTo[S, p]]
    ];
    Hi = Subgroup[{1}, S];
    If[!MemberQ[H, Hi], AppendTo[H, Hi]]
  ];
  t[1] = Length[H];
  For[i = 2, i <= t[1] - 1, i++,
    Hi = Part[H, i];
    For[j = i + 1, j <= t[1], j++,
      Hj = Part[H, j];
      Hij = If[Length[Hi] >= Length[Hj], Subgroup[Hi, Hj], Subgroup[Hj, Hi]];
      If[!MemberQ[H, Hij], AppendTo[H, Hij]]
    ]
  ];
  t[2] = Length[H];
  For[k = 3, t[k - 1] > t[k - 2], k++,
    For[i = t[k - 2] + 1, i <= t[k - 1], i++,
      Hi = Part[H, i];
      For[j = 2, j <= t[1], j++,
        Hj = Part[H, j];
        Hij = If[Length[Hi] >= Length[Hj], Subgroup[Hi, Hj], Subgroup[Hj, Hi]];
        If[!MemberQ[H, Hij], AppendTo[H, Hij]]
      ]
    ];
    t[k] = Length[H]
  ];
];
```

ここで

$t[k]$: k 個以下の元から生成される正規部分群の個数

《サブプログラム(3)》

ガロア群Gの組成列Gsを求める。

```
(* Composition Series of Galois Group *)
CompositionSeries[]:=Module[{Gk,Gkm1,i,L},
  Gs={};
  Gkm1=Table[i,{i,1,nn}];
  AppendTo[Gs,Gkm1];
  While[True,
    AllNormalSubgroups[Gkm1];
    Gk={1};
    For[i=1,i<=Length[H],i++,
      L=Length[Part[H,i]];
      If[Length[Gkm1]>L && L>Length[Gk],Gk=Part[H,i]]
    ];
    AppendTo[Gs,Gk];
    If[Length[Gk]==1,Break[],Gkm1=Gk]
  ]
];
```

《メインプログラム》

```
n=4;
nn=Factorial[n];
G=Permutations[Table[i,{i,1,n}]];
ProductOfG[];
InverseOfG[];
CompositionSeries[];
For[i=1,i<=Length[Gs],i++,
  Print["G",i-1,"=",Part[Gs,i]]
];
```

《計算結果》

```
G0={1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24}
G1={1,4,5,8,9,12,13,16,17,20,21,24}
G2={1,8,17,24}
G3={1,8}
G4={1}
```

10. 数式処理ソフトによる計算

第1部で示したプログラムを1つにまとめて、計算結果をファイルに書き込むようにした。

《サブプログラム》

計算結果をファイルに書き込む。

```
(* Write Results into File *)
WriteFile[FileName_] := Module[{fp, i},
  fp = OpenWrite[FileName];
  WriteString[fp, "fx=", InputForm[fx], ";¥n"];
  For[i = 1, i <= n, i++,
    WriteString[fp, "m[" , i, "]=", m[i], ";¥n"]
  ];
  WriteString[fp, "gx=", InputForm[gx], ";¥n"];
  For[i = 1, i <= n, i++,
    WriteString[fp, "X[" , i, "]=", InputForm[X[i]], ";¥n"]
  ];
  WriteString[fp, "G=", G, ";¥n"];
  WriteString[fp, "Gs=", Gs, ";¥n"];
  Close[fp]
];
```

ここで

fp=OpenWrite[file] : 出力ファイルfileを開く。

WriteString[fp, f] : ファイルに数式fを書き込む。

InputForm[f] : 数式fを入力形式で表す。

例えば, $f = \sqrt{1+x^2}$ ならば, InputForm[f]はSqrt[1+x^2]となる。

Close[fp] : ファイルを閉じる。

《メインプログラム》

```
(* Calculation of Galois Group of f(x) *)
fx = Input["f(x)="];
n = Exponent[fx, x];
nn = Factorial[n];
RelationsOfX[fx];
sigma = Permutations[Table[i, {i, 1, n}]];
PrimitiveElement[];
MinimalPolynomial[];
Print["g(x)=", gx];
BasisOfSplittingField[];
PowerOfV[];
XOfV[];
For[i = 1, i <= n, i++,
  Print["X[" , i, "]=", X[i]]
];
```

```

];
GaloisGroup[];
Print["G=", G];
ProductOfG[];
InverseOfG[];
CompositionSeries[];
For[i=1, i<=Length[Gs], i++,
  Print["G", i-1, "=", Part[Gs, i]];
  sol=If[i==1, True, sol && PrimeQ[Length[Part[Gs, i-1]]/Length[Part[Gs, i]]]]
];
Print["f(x) is ", If[sol, "", "not "], "solvable. "];
SetDirectory["C:\Users\Myname\Documents\Mathematica"];
FileName=InputString["Output file name : "];
WriteFile[FileName];

```

ここで

PrimeQ[n] : nが素数ならば真, そうでなければ偽とする。

SetDirectory[dir] : カレントディレクトリをdirに設定する。

InputString[prompt] : 入力要求promptを表示して文字列を入力する。

(注意) SetDirectory中の"C:\Users...Mathematica"は, 実際にファイルを置く場所書き換える。

《計算結果》

$f(x)=x^3+a_2x^2+a_1x+a_0$ の計算結果を示す。入力要求"f(x)="に対して" $x^3+a_2x^2+a_1x+a_0$ "を入力する。

```

m[1]=1
m[2]=-1
m[3]=0
g(x)=27a0^2+4a1^3-18a0 a1 a2-a1^2a2^2+4a0 a2^3+9a1^2x^2-6a1 a2^2x^2+a2^4x^2+6a1 x^4-2a2^2x^4+x^6
X[1]=(12a1^2-18a0 a2-2a1 a2^2+27a0 v-9a1 a2 v+2a2^3v+15a1 v^2-5a2^2v^2+3v^4)/
(54a0-18a1 a2+4a2^3)
X[2]=(12a1^2-18a0 a2-2a1 a2^2-27a0 v+9a1 a2 v-2a2^3v+15a1 v^2-5a2^2v^2+3v^4)/
(54a0-18a1 a2+4a2^3)
X[3]=(12a1^2+9a0 a2-11a1 a2^2+2a2^4+15a1 v^2-5a2^2v^2+3v^4)/(-27a0+9a1 a2-2a2^3)
G={ {1, 2, 3}, {1, 3, 2}, {2, 1, 3}, {2, 3, 1}, {3, 1, 2}, {3, 2, 1} }
G0={1, 2, 3, 4, 5, 6}
G1={1, 4, 5}
G2={1}
f(x) is solvable.

```

入力要求"Output file name : "に対して"example1.txt"を入力すると, ファイルexample1.txtに以下の計算結果が書き込まれる。

```

fx=a0+a1*x+a2*x^2+x^3;
m[1]=1;
m[2]=-1;
m[3]=0;

```

$$\begin{aligned}
&gx=27*a0^2+4*a1^3-18*a0*a1*a2-a1^2*a2^2+4*a0*a2^3+9*a1^2*x^2- \\
&\quad 6*a1*a2^2*x^2+a2^4*x^2+6*a1*x^4-2*a2^2*x^4+x^6; \\
&X[1]=(12*a1^2-18*a0*a2-2*a1*a2^2+27*a0*v-9*a1*a2*v+2*a2^3*v+ \\
&\quad 15*a1*v^2-5*a2^2*v^2+3*v^4)/(54*a0-18*a1*a2+4*a2^3); \\
&X[2]=(12*a1^2-18*a0*a2-2*a1*a2^2-27*a0*v+9*a1*a2*v-2*a2^3*v+ \\
&\quad 15*a1*v^2-5*a2^2*v^2+3*v^4)/(54*a0-18*a1*a2+4*a2^3); \\
&X[3]=(12*a1^2+9*a0*a2-11*a1*a2^2+2*a2^4+15*a1*v^2-5*a2^2*v^2+ \\
&\quad 3*v^4)/(-27*a0+9*a1*a2-2*a2^3); \\
&G=\{ \{1, 2, 3\}, \{1, 3, 2\}, \{2, 1, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{3, 2, 1\} \}; \\
&Gs=\{ \{1, 2, 3, 4, 5, 6\}, \{1, 4, 5\}, \{1\} \};
\end{aligned}$$

上記の計算結果も含めて、以下に9つの計算例(計算不可の場合も含む)を示す。

(例1) $f(x)=x^3+a_2x^2+a_1x+a_0$ の場合

$$v=x_1-x_2 \quad (10.1)$$

$$g(x)=x^6+2(3a_1-a_2^2)x^4+(9a_1^2-6a_1a_2^2+a_2^4)x^2+27a_0^2+4a_1^3-18a_0a_1a_2-a_1^2a_2^2+4a_0a_2^3 \quad (10.2)$$

$$x_1=\{3v^4+5(3a_1-a_2^2)v^2+(27a_0-9a_1a_2+2a_2^3)v+2(6a_1^2-9a_0a_2-a_1a_2^2)\}/2D \quad (10.3)$$

$$x_2=\{3v^4+5(3a_1-a_2^2)v^2-(27a_0-9a_1a_2+2a_2^3)v+2(6a_1^2-9a_0a_2-a_1a_2^2)\}/2D \quad (10.4)$$

$$x_3=\{-3v^4-5(3a_1-a_2^2)v^2-12a_1^2-9a_0a_2+11a_1a_2^2-2a_2^4\}/D \quad (10.5)$$

$$D=27a_0-9a_1a_2+2a_2^3 \quad (10.6)$$

$$G=\{ \{1, 2, 3\}, \{1, 3, 2\}, \{2, 1, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{3, 2, 1\} \} \quad (10.7)$$

$$G_0=\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}, \quad G_1=\{\sigma_1, \sigma_4, \sigma_5\}, \quad G_2=\{\sigma_1\} \quad (10.8)$$

(例2) $f(x)=x^4+a_2x^2+a_0$ の場合

$$v=x_1+2x_2-2x_3 \quad (10.9)$$

$$g(x)=x^8+10a_2x^6-(14a_0-33a_2^2)x^4-10a_2(7a_0-4a_2^2)x^2+(25a_0-4a_2^2)^2 \quad (10.10)$$

$$x_1=\{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3-(4750a_0^2-3945a_0a_2^2+308a_2^4)v\}/D \quad (10.11)$$

$$x_2=-\{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3-(4750a_0^2-3945a_0a_2^2+308a_2^4)v\}/D \quad (10.12)$$

$$x_3=-\{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3+(10250a_0^2+195a_0a_2^2-92a_2^4)v\}/2D \quad (10.13)$$

$$x_4=\{7a_2v^7+10(25a_0+3a_2^2)v^5+a_2(1777a_0-69a_2^2)v^3+(10250a_0^2+195a_0a_2^2-92a_2^4)v\}/2D \quad (10.14)$$

$$D=6(25a_0-4a_2^2)(100a_0-9a_2^2) \quad (10.15)$$

$$G=\{ \{1, 2, 3, 4\}, \{1, 2, 4, 3\}, \{2, 1, 3, 4\}, \{2, 1, 4, 3\}, \{3, 4, 1, 2\}, \{3, 4, 2, 1\}, \\ \{4, 3, 1, 2\}, \{4, 3, 2, 1\} \} \quad (10.16)$$

$$G_0=\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8\}, \quad G_1=\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}, \quad G_2=\{\sigma_1, \sigma_2\}, \quad G_3=\{\sigma_1\} \quad (10.17)$$

(例3) $f(x)=x^4+a_2x^2+a_1x+a_0$ の場合

$$v=x_1-x_2+2x_3 \quad (10.18)$$

$$\begin{aligned}
g(x)=&x^{24}+40a_2x^{22}-4(20a_0-171a_2^2)x^{20}+20(17a_1^2-136a_0a_2+330a_2^3)x^{18}+2(3760a_0^2+4636a_1^2a_2-19448a_0a_2^2 \\
&+19995a_2^4)x^{16}+20(1156a_0a_1^2+7968a_0^2a_2+5147a_1^2a_2^2-15088a_0a_2^3+8010a_2^5)x^{14}-2(553600a_0^3-66911a_1^4 \\
&+30016a_0a_1^2a_2-861344a_0^2a_2^2-314656a_1^2a_2^3+711128a_0a_2^4-217590a_2^6)x^{12}-20(23120a_0^2a_1^2+659840a_0^3a_2 \\
&-87054a_1^4a_2+160392a_0a_1^2a_2^2-514592a_0^2a_2^3-117767a_1^2a_2^4+216520a_0a_2^5-40470a_2^7)x^{10}+(49475840a_0^4 \\
&+1423440a_0a_1^4+9624960a_0^2a_1^2a_2-76089600a_0^3a_2^2+8760420a_1^4a_2^2-19828160a_0a_1^2a_2^3+35380320a_0^2a_2^4 \\
&+5556632a_1^2a_2^5-8711056a_0a_2^6+1027665a_2^8)x^8+20(3381440a_0^3a_1^2+328077a_1^6+12301312a_0^4a_2-742536a_0a_1^4a_2 \\
&+4560752a_0^2a_1^2a_2^2-10712064a_0^3a_2^3+1129090a_1^4a_2^3-2718812a_0a_1^2a_2^4+3486592a_0^2a_2^5+407357a_1^2a_2^6-569152a_0a_2^7 \\
&+43700a_2^9)x^6-2(172244992a_0^5-206131824a_0^2a_1^4+272813568a_0^3a_1^2a_2-20518596a_1^6a_2-309948416a_0^4a_2^2
\end{aligned}$$

$$\begin{aligned}
&+67415544a_0a_1^4a_2^2-176732800a_0^2a_1^2a_2^3+165791744a_0^3a_2^4-16669527a_1^4a_2^4+40474272a_0a_1^2a_2^5-39351808a_0^2a_2^6 \\
&-3564856a_1^2a_2^7+4597568a_0a_2^8-237872a_2^{10})x^4-20(-104730624a_0^4a_1^2-1000188a_0a_1^6+39124992a_0^5a_2 \\
&-47500992a_0^2a_1^4a_2+84363264a_0^3a_1^2a_2^2-3369681a_1^6a_2^2-36847616a_0^4a_2^3+11854944a_0a_1^4a_2^3-24342528a_0^2a_1^2a_2^4 \\
&+13443072a_0^3a_2^5-1303596a_1^4a_2^5+3128192a_0a_1^2a_2^6-2377728a_0^2a_2^7-169712a_1^2a_2^8+207104a_0a_2^9-7488a_2^{11})x^2 \\
&+(25600a_0^3-9261a_1^4+22176a_0a_1^2a_2-15104a_0^2a_2^2-2344a_1^2a_2^3+2752a_0a_2^4-144a_2^6)^2 \quad (10.19)
\end{aligned}$$

x_1, x_2, x_3, x_4 は長い式になるため省略する。

$$\begin{aligned}
G = &\{\{1, 2, 3, 4\}, \{1, 2, 4, 3\}, \{1, 3, 2, 4\}, \{1, 3, 4, 2\}, \{1, 4, 2, 3\}, \{1, 4, 3, 2\}, \\
&\{2, 1, 3, 4\}, \{2, 1, 4, 3\}, \{2, 3, 1, 4\}, \{2, 3, 4, 1\}, \{2, 4, 1, 3\}, \{2, 4, 3, 1\}, \\
&\{3, 1, 2, 4\}, \{3, 1, 4, 2\}, \{3, 2, 1, 4\}, \{3, 2, 4, 1\}, \{3, 4, 1, 2\}, \{3, 4, 2, 1\}, \\
&\{4, 1, 2, 3\}, \{4, 1, 3, 2\}, \{4, 2, 1, 3\}, \{4, 2, 3, 1\}, \{4, 3, 1, 2\}, \{4, 3, 2, 1\}\} \quad (10.20)
\end{aligned}$$

$$\begin{aligned}
G_0 = &\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}, \sigma_{17}, \sigma_{18}, \sigma_{19}, \sigma_{20}, \sigma_{21}, \sigma_{22}, \sigma_{23}, \sigma_{24}\} \\
G_1 = &\{\sigma_1, \sigma_4, \sigma_5, \sigma_8, \sigma_9, \sigma_{12}, \sigma_{13}, \sigma_{16}, \sigma_{17}, \sigma_{20}, \sigma_{21}, \sigma_{24}\} \\
G_2 = &\{\sigma_1, \sigma_8, \sigma_{17}, \sigma_{24}\}, \quad G_3 = \{\sigma_1, \sigma_8\}, \quad G_4 = \{\sigma_1\} \quad (10.21)
\end{aligned}$$

(例4) $f(x)=x^4+2x^3+3x^2+4x+5$ の場合

$$v=x_1-x_2+2x_3 \quad (10.22)$$

$$\begin{aligned}
g(x) = &x^{24}+24x^{23}+336x^{22}+3344x^{21}+25740x^{20}+159984x^{19}+820856x^{18}+3519504x^{17}+12721926x^{16} \\
&+39075680x^{15}+104485896x^{14}+257189424x^{13}+603068156x^{12}+1264487184x^{11}+1484791560x^{10} \\
&-3707413456x^9-23515353279x^8-53513746296x^7-7075256024x^6+299352120960x^5 \\
&+770653544880x^4+869309952000x^3+1145273500800x^2+1451723788800x \\
&+1818528595200 \quad (10.23)
\end{aligned}$$

$$\begin{aligned}
x_1 = &(-208353677612355954546433162v^{23}-4700469602045680704907486053v^{22} \\
&-62743978205081535599780037425v^{21}-597414837578128461452430220879v^{20} \\
&-4398641079449678165326681214688v^{19}-26145596673787674379554463882109v^{18} \\
&-128043645421283572717320394479247v^{17}-522884391088876462622539107412839v^{16} \\
&-1800854692663314698641992078879746v^{15}-5297080327431065950428005125610863v^{14} \\
&-13863703895775340309824222856236831v^{13}-34905331377756025440724893423199157v^{12} \\
&-84361546562095885356604777317104356v^{11}-174259119004940368313420310312516375v^{10} \\
&-160357808657260211836473293844892817v^9+700852019454854027355247003047909467v^8 \\
&+2832521992294377321078352663850262192v^7+3850487113957148789514185107746029800v^6 \\
&-7601468081023869713051291841551352240v^5-48665928754463279546704919618458282992v^4 \\
&-47611440099613383846062249354627809920v^3-29497809558305091774143086058536905600v^2 \\
&-347848807313865406628952035803916824320v-344977446038238726659287243238508560640) \\
&/301116866499846787840952406238385602560 \quad (10.24)
\end{aligned}$$

$$\begin{aligned}
x_2 = &(-208353677612355954546433162v^{23}-5067129534199705703549392745v^{22} \\
&-70810496712470085569901984649v^{21}-695691640735763991382928333551v^{20} \\
&-5234864551567991768119570856768v^{19}-31392456125941987107152792012473v^{18} \\
&-152905966814157702600330137167687v^{17}-607831957458341826814573920624767v^{16} \\
&-1967468827511539542752350315901698v^{15}-5142421485106444550477819036247787v^{14} \\
&-11028330649734739045612660050541799v^{13}-21906879364136908571603265844308709v^{12} \\
&-46862651360934910597323801030968452v^{11}-78163814216064425824612171051077467v^{10} \\
&+154485577574836214112087042501435335v^9+1839512255065178882667267833419269443v^8 \\
&+617660660592005357241036223965877760v^7+6365549973582078490057044489539889512v^6 \\
&-24548819784172573880250751621909193520v^5-96798920419628677195780007067848367216v^4 \\
&-92602735718572166795529968365122514560v^3+298838110245729036086488027851460252800v^2 \\
&+33513555124905980032912458332196092160v-1135910483993622438918429576588629694720) \\
&/903350599499540363522857218715156807680 \quad (10.25)
\end{aligned}$$

$$\begin{aligned}
x_3 = & (208353677612355954546433162v^{23} + 4517139635968668205586532707v^{22} \\
& + 58710718951387260614719063813v^{21} + 548276435999310696487181164543v^{20} \\
& + 3980529343390521363930236393648v^{19} + 23522166947710518015755299816927v^{18} \\
& + 115612484724846507775815523135027v^{17} + 480410607904143780526521700806875v^{16} \\
& + 1717547625239202276586812960368770v^{15} + 5374409748593376650403098170292401v^{14} \\
& + 15281390518795640941930004259084347v^{13} + 41404557384565583875285707212644381v^{12} \\
& + 103110994162676372736245265460172308v^{11} + 222306771399378339557824379943235829v^{10} \\
& + 317779501773308424810753462018056893v^9 - 131521901649691599699236587862229479v^8 \\
& - 1160479685481539195412347875945999408v^7 - 2592955684144683939242755416849099944v^6 \\
& - 872207770550482370548438048627568400v^5 + 24599432921880580722167375893763240880v^4 \\
& + 25115792290133992371328389849380457600v^3 + 193665769460322155704458643013535484800v^2 \\
& + 990205288283021281721312892229551686400v - 50489072939453129470283923436552006400) \\
& / 903350599499540363522857218715156807680
\end{aligned} \tag{10.26}$$

$$\begin{aligned}
x_4 = & (208353677612355954546433162v^{23} + 4883799568122693204228439399v^{22} \\
& + 66777237458775810584841011037v^{21} + 646553239156946226417679277215v^{20} \\
& + 4816752815508834966723126035728v^{19} + 28769026399864830743353627947291v^{18} \\
& + 140474806117720637658825265823467v^{17} + 565358174273609144718556514018803v^{16} \\
& + 1884161760087427120697171197390722v^{15} + 5219750906268755250452912080929325v^{14} \\
& + 12446017272755039677718441453389315v^{13} + 28406105370946467006164079633753933v^{12} \\
& + 65612098961515397976964289174036404v^{11} + 126211466610502397069016240681796921v^{10} \\
& + 2936115541211998862193125671728741v^9 - 1270182137260016455011257418233589455v^8 \\
& - 4504564299107215446744357451754524976v^7 - 5108018543769613639785614798642959656v^6 \\
& + 16075143932598221796651021731730272880v^5 + 72732424587045978371242463343153325104v^4 \\
& + 70107087909092775320796108859875162240v^3 - 134670150343711972156172470896461673600v^2 \\
& + 6609192844556319377543585616667564800v + 138210232016237007106953597436797922560) \\
& / 301116866499846787840952406238385602560
\end{aligned} \tag{10.27}$$

$$\begin{aligned}
G = & \{ \{1, 2, 3, 4\}, \{1, 2, 4, 3\}, \{1, 3, 2, 4\}, \{1, 3, 4, 2\}, \{1, 4, 2, 3\}, \{1, 4, 3, 2\}, \\
& \{2, 1, 3, 4\}, \{2, 1, 4, 3\}, \{2, 3, 1, 4\}, \{2, 3, 4, 1\}, \{2, 4, 1, 3\}, \{2, 4, 3, 1\}, \\
& \{3, 1, 2, 4\}, \{3, 1, 4, 2\}, \{3, 2, 1, 4\}, \{3, 2, 4, 1\}, \{3, 4, 1, 2\}, \{3, 4, 2, 1\}, \\
& \{4, 1, 2, 3\}, \{4, 1, 3, 2\}, \{4, 2, 1, 3\}, \{4, 2, 3, 1\}, \{4, 3, 1, 2\}, \{4, 3, 2, 1\} \}
\end{aligned} \tag{10.28}$$

$$\begin{aligned}
G_0 = & \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}, \sigma_{17}, \sigma_{18}, \sigma_{19}, \sigma_{20}, \sigma_{21}, \sigma_{22}, \sigma_{23}, \sigma_{24}\} \\
G_1 = & \{\sigma_1, \sigma_4, \sigma_5, \sigma_8, \sigma_9, \sigma_{12}, \sigma_{13}, \sigma_{16}, \sigma_{17}, \sigma_{20}, \sigma_{21}, \sigma_{24}\} \\
G_2 = & \{\sigma_1, \sigma_8, \sigma_{17}, \sigma_{24}\}, \quad G_3 = \{\sigma_1, \sigma_8\}, \quad G_4 = \{\sigma_1\}
\end{aligned} \tag{10.29}$$

(例5) $f(x) = x^5 + 2x^3 + 4x^2 - x + 4$ の場合

$$v = x_1 - x_2 + 2x_3 - 2x_4 \tag{10.30}$$

$$\begin{aligned}
g(x) = & x^{20} + 100x^{18} + 1298x^{16} - 82900x^{14} - 324031x^{12} + 58499280x^{10} - 1752946672x^8 \\
& + 27826563840x^6 - 165874705856x^4 + 328635141120x^2 + 112239429632
\end{aligned} \tag{10.31}$$

x_1, x_2, x_3, x_4, x_5 は長い式になるため省略する。

$$\begin{aligned}
G = & \{ \{1, 2, 3, 4, 5\}, \{1, 3, 2, 5, 4\}, \{1, 4, 5, 3, 2\}, \{1, 5, 4, 2, 3\}, \{2, 1, 4, 3, 5\}, \\
& \{2, 3, 5, 4, 1\}, \{2, 4, 1, 5, 3\}, \{2, 5, 3, 1, 4\}, \{3, 1, 5, 2, 4\}, \{3, 2, 4, 5, 1\}, \\
& \{3, 4, 2, 1, 5\}, \{3, 5, 1, 4, 2\}, \{4, 1, 3, 5, 2\}, \{4, 2, 5, 1, 3\}, \{4, 3, 1, 2, 5\}, \\
& \{4, 5, 2, 3, 1\}, \{5, 1, 2, 4, 3\}, \{5, 2, 1, 3, 4\}, \{5, 3, 4, 1, 2\}, \{5, 4, 3, 2, 1\} \}
\end{aligned} \tag{10.32}$$

$$\begin{aligned}
G_0 = & \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}, \sigma_{17}, \sigma_{18}, \sigma_{19}, \sigma_{20}\} \\
G_1 = & \{\sigma_1, \sigma_2, \sigma_5, \sigma_7, \sigma_9, \sigma_{12}, \sigma_{14}, \sigma_{16}, \sigma_{19}, \sigma_{20}\}, \quad G_2 = \{\sigma_1, \sigma_7, \sigma_9, \sigma_{16}, \sigma_{19}\}, \quad G_3 = \{\sigma_1\}
\end{aligned} \tag{10.33}$$

$|G_0/G_1|=2, \quad |G_1/G_2|=2, \quad |G_2/G_3|=5$ はすべて素数であるから、 $f(x)$ は可解である。

(例6) $f(x)=x^5+a_3x^3+(a_3^2/5)x+a_0$ の場合

$$v=x_1-x_2+2x_3-2x_4 \quad (10.34)$$

$$\begin{aligned} g(x)= & x^{20}+50a_3x^{18}+1025a_3^2x^{16}+11250a_3^3x^{14}+72500a_3^4x^{12}+625(3125a_0^2+454a_3^5)x^{10} \\ & +625a_3(43750a_0^2+1081a_3^5)x^8+6250a_3^2(21875a_0^2+153a_3^5)x^6 \\ & +15625a_3^3(18750a_0^2+49a_3^5)x^4+78125a_3^4(3125a_0^2+4a_3^5)x^2+3125(3125a_0^2+4a_3^5)^2 \end{aligned} \quad (10.35)$$

$g(x)$ の計算まではできたが、それより後の計算はできなかった。

(例7) $f(x)=x^5+2x^4+3x^3+4x^2+5x+6$ の場合

$$v=x_1-x_2+2x_3-2x_4 \quad (10.36)$$

$$\begin{aligned} g(x)= & x^{120}+420x^{118}+82866x^{116}+10199840x^{114}+875163471x^{112}+55232462880x^{110}+2626965601806x^{108} \\ & +94241569949100x^{106}+2454636314062611x^{104}+37880980352537560x^{102}-328425910494720528x^{100} \\ & -57006637719320887080x^{98}-3154847604920171825224x^{96}-133696456889358231064560x^{94} \\ & -4576413527484539483173284x^{92}-118350570675607278229265520x^{90}-1612044959450149752998131179x^{88} \\ & +42213759494677875028385099100x^{86}+3746004268227090255499260100786x^{84} \\ & +123685837343622132519496477306560x^{82}+1584591265304015950418478171756969x^{80} \\ & -34599383449964061459344391855769720x^{78}-175175922244173101964146103927510286x^{76} \\ & -17260156048718480840353156518281830860x^{74}+546088799265339179977098353845271343486x^{72} \\ & +18610786817926133877872453408903356460940x^{70}+261014019175791551676059499901871540833506x^{68} \\ & +5229395181676456782203730698918753090929280x^{66} \\ & +116791575458330264100173712528316594741397721x^{64} \\ & -1790031340891099581276145244833056275629625640x^{62} \\ & -162916942653267076663168362831426721870961764718x^{60} \\ & -3305869134127681286557973232854645227820969920980x^{58} \\ & -721437846948686409860246317127584989144229195995x^{56} \\ & +892416134219498091898071285200014387380027114879720x^{54} \\ & +19207108997085576049608590525509925145163955221123692x^{52} \\ & +149827588497925540873632892204733715663580287614529120x^{50} \\ & -693643435390570162649633317405684307595553454984536744x^{48} \\ & -47029235376462385026532166017149412578382908303929791560x^{46} \\ & -647119283760045163682196508551060339189927475237284633024x^{44} \\ & -1425210914860400711198136344709459726609648864011286373040x^{42} \\ & +79470092697141328970203619628692060511749124704281205089443x^{40} \\ & +762163377930258045336868770798704835849779267038313593144620x^{38} \\ & -8117646002890523200559247070428889510914176274980991831525522x^{36} \\ & -199514113242417023593067010972647553097476036885127872544294680x^{34} \\ & -1326778789347435537656438178154814675335463398857615091665054465x^{32} \\ & -7550572712650455548140812926381924431910229187979928166951380040x^{30} \\ & +443202954199490916618052115076366116917935272691180861153838931154x^{28} \\ & +7359891041597830714789359039792295523065249590845880020378100363540x^{26} \\ & +25405243241148399506382633258517993867050897768909772229826229587121x^{24} \\ & +33661661028026402444122369224964887071628372030423587028692067348360x^{22} \\ & +1090734999122458699620193594757425502950290430819258811672404012056048x^{20} \\ & +3376506862285724258835953628567969719895213537352221267771067062253440x^{18} \\ & -21000875523747163548238695270279722787146079479998568583293076683529984x^{16} \\ & -49676509720280507312348270675342052234240026038711490446304129577615360x^{14} \\ & +135499741498483774696205987825411442454974384950055978100155649450967040x^{12} \\ & +161369262632985697633276479090202520190481664567304254877249118226350080x^{10} \\ & +98356077450927450744136719968814324524566726518658065409357935103967232x^8 \\ & -1555853199128822941506205075420779261574025148370312187670106160140124160x^6 \end{aligned}$$

$$\begin{aligned}
&+1423799218936084461930191063078865007518762296478040243673086544786227200x^4 \\
&+203751572639989342709533904694884192532399532846330562484910833008640x^2 \\
&+1848649792819529877238239584136719252230295418813286057423065317376 \quad (10.37)
\end{aligned}$$

x_1, x_2, x_3, x_4, x_5 は長い式になるため省略する。 G は5根の置換のすべて(計120個)からなる。組成列を $G=G_0 \supset G_1 \supset G_2$ とすると, G_1 は偶置換(計60個), G_2 は単位群である。 $|G_1/G_2|=60$ は素数ではないから, $f(x)$ は可解ではない。

(例8) $f(x)=x^6+2x^5+3x^4+4x^3+5x^2+6x+7$ の場合

いくつかの難関があつて, 計算するのは到底不可能である。

- (1) $v=x_1-x_2+2x_3-2x_4+3x_5$ とすると, (4.2)の $g(x)$ は計算できたが, この720次多項式の定数項は504桁にもなり, これに続く $g(x)$ の因数分解の計算は終わることができなかった。
 - (2) $g(x)$ の因数分解の計算は断念して($g(x)$ は既約であつたと仮定する), (6.1)の右辺の係数行列(720行 $\times$ 720列)の計算を始めたが, これも終わることができなかった。係数行列のサイズが大きだけでなく, 数百桁になる要素もあつて, 非常に重い計算となる。
 - (3) この係数行列が計算できたと仮定しても, これに続く720元連立1次方程式の計算 —— $x_1, x_2, x_3, x_4, x_5, x_6$ の v による多項式表現を求める。—— は終わることができないであろうと予想される。
 - (4) $f(x)$ のガロア群は6次対称群になると仮定して, その組成列を計算することはできた。
- (追記) 後でわかったことであるが, 意外にも $g(x)$ は6個の120次多項式の積に分解できる。

(例9) $f(x)=x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$ の場合

これは1の原始17乗根を求める方程式である。本節のプログラムでは計算できないが, 以下のようになることが知られている。

$$v=x_1 \quad (10.38)$$

$$g(x)=f(x) \quad (10.39)$$

$$x_1=v, x_2=v^2, \dots, x_{15}=v^{15} \quad (10.40)$$

$$x_{16}=-(v^{15}+v^{14}+v^{13}+v^{12}+v^{11}+v^{10}+v^9+v^8+v^7+v^6+v^5+v^4+v^3+v^2+v+1) \quad (10.41)$$

x_i を x_{3i} (3iは17を法とする)に移す置換を τ とし, これまでと同じく $x_1, x_2, \dots, x_{16}$ を $x_{j_1}, x_{j_2}, \dots, x_{j_{16}}$ に移す置換を $\{j_1, j_2, \dots, j_{16}\}$ で表すと, τ は以下のように表される。

$$\tau=\{3, 6, 9, 12, 15, 1, 4, 7, 10, 13, 16, 2, 5, 8, 11, 14\} \quad (10.42)$$

このとき, ガロア群 G は以下の16個の置換となる。

$$\begin{aligned}
G &= \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}\} \\
&= \{\tau^0, \tau^1, \tau^2, \tau^3, \tau^4, \tau^5, \tau^6, \tau^7, \tau^8, \tau^9, \tau^{10}, \tau^{11}, \tau^{12}, \tau^{13}, \tau^{14}, \tau^{15}\} \quad (10.43)
\end{aligned}$$

その組成列は次式となる。

$$\begin{aligned}
G_0 &= \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}\} \\
G_1 &= \{\sigma_1, \sigma_3, \sigma_5, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{15}\}, \quad G_2 = \{\sigma_1, \sigma_5, \sigma_9, \sigma_{13}\}, \quad G_3 = \{\sigma_1, \sigma_9\}, \quad G_4 = \{\sigma_1\} \quad (10.44)
\end{aligned}$$

$|G_0/G_1|=2, |G_1/G_2|=2, |G_2/G_3|=2, |G_3/G_4|=2$ はすべて素数であるから, $f(x)$ は可解である。

11. $f(x)$ の分解体に属する元の表記と積・商の計算

これより後は可解な代数方程式の解法について述べるので、ガロア群 G は可解であるとする。ガロア群 G の組成列 (9. 1) に対応する体の拡大を次式とする。

$$F_0 \subset F_1 \subset \cdots \subset F_s \quad (11.1)$$

ここで、 F_0 は $f(x)$ の係数体、 F_s は $f(x)$ の分解体である。 k 番目の組成列 $G_{k-1} \supset G_k$ とこれに対応する体の拡大 $F_{k-1} \subset F_k$ において、 $|G_{k-1}/G_k| = p_k$ (素数)、1 の原始 p_k 乗根を ζ_{p_k} とする。 F_{k-1} の元と ζ_{p_k} との四則演算で作られる1つの数を A_k とし (詳しい計算方法は後述する)、その p_k 乗根を $\alpha_k = \sqrt[p_k]{A_k}$ とすると、 F_{k-1} に α_k を付加してできる体が F_k となる。 α_k は k 重のべき根で表されるから、そのまま表記すると長い式になってしまう。このため、今後は文字 α_k のままで表記する。同様に、 ζ_{p_k} も $p_k \geq 3$ の場合は文字 ζ_{p_k} のままで表記する。このようにすると、 F_k の元は $\alpha_1, \alpha_2, \dots, \alpha_k$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_k}$ の多項式で表される。ただし、 α_k には次式が成り立つから、 α_k の次数は $p_k - 1$ 以下となる。

$$\alpha_k^{p_k} - A_k = 0 \quad (11.2)$$

また、 ζ_{p_k} には次式が成り立つから、 ζ_{p_k} の次数は $p_k - 2$ 以下となる。

$$\zeta_{p_k}^{p_k-1} + \cdots + \zeta_{p_k} + 1 = 0 \quad (11.3)$$

以上より、 $f(x)$ の分解体 F_s に属する2つの元を P, Q とし、積 PQ を求める方法を示す。まず、積 PQ をふつうに $\alpha_1, \alpha_2, \dots, \alpha_s$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_s}$ の多項式として求める。ここで、 α_k の次数が p_k 以上となった場合は、(11.2) による剰余を取り、 α_k の次数を $p_k - 1$ 以下に低減させる。 ζ_{p_k} の次数が $p_k - 1$ 以上となった場合は、(11.3) による剰余を取り、 ζ_{p_k} の次数を $p_k - 2$ 以下に低減させる。ただし、 α_k の次数低減については、 A_k は $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_k}$ の多項式であるから、(11.2) による剰余を取ることで、 $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_k}$ の次数が変わってしまう。よって、 $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_k}$ の次数低減は、 α_k の次数低減より後に行うようにしなければならない。したがって、次数低減は $\alpha_s, \zeta_{p_s}, \dots, \alpha_2, \zeta_{p_2}, \alpha_1, \zeta_{p_1}$ の順序で行うことにする。

(例1) $s=2, p_1=2, p_2=3, \alpha_1^2+6=0, \alpha_2^3-3(1+\alpha_1+2\zeta_3)=0$ の場合

$P=3\alpha_2+2\alpha_1\alpha_2^2-3\alpha_2\zeta_3-3\alpha_2^2\zeta_3+\alpha_1\alpha_2^2\zeta_3, Q=3-\alpha_2-\alpha_1\alpha_2+\alpha_2\zeta_3-\alpha_1\alpha_2\zeta_3-\alpha_2^2\zeta_3$ とし、積 PQ を求める。まず、積をふつうに α_1, α_2 および ζ_3 の多項式として求める。

$$\begin{aligned} PQ = & 9\alpha_2-3\alpha_2^2+3\alpha_1\alpha_2^2-2\alpha_1\alpha_2^3-2\alpha_1^2\alpha_2^3-9\alpha_2\zeta_3-3\alpha_2^2\zeta_3+3\alpha_1\alpha_2^2\zeta_3+4\alpha_1\alpha_2^3\zeta_3-3\alpha_1^2\alpha_2^3\zeta_3 \\ & -2\alpha_1\alpha_2^4\zeta_3-3\alpha_2^2\zeta_3^2+3\alpha_1\alpha_2^2\zeta_3^2+4\alpha_1\alpha_2^3\zeta_3^2-\alpha_1^2\alpha_2^3\zeta_3^2+3\alpha_2^4\zeta_3^2-\alpha_1\alpha_2^4\zeta_3^2 \end{aligned} \quad (11.4)$$

$\alpha_2^3-3(1+\alpha_1+2\zeta_3)$ による剰余を取り、 α_2 の次数を2以下に低減させる。

$$\begin{aligned} PQ = & -6\alpha_1-12\alpha_1^2-6\alpha_1^3+9\alpha_2-3\alpha_2^2+3\alpha_1\alpha_2^2-9\alpha_1^2\zeta_3-9\alpha_1^3\zeta_3-9\alpha_2\zeta_3-6\alpha_1\alpha_2\zeta_3-6\alpha_1^2\alpha_2\zeta_3 \\ & -3\alpha_2^2\zeta_3+3\alpha_1\alpha_2^2\zeta_3+36\alpha_1\zeta_3^2-9\alpha_1^2\zeta_3^2-3\alpha_1^3\zeta_3^2+9\alpha_2\zeta_3^2-6\alpha_1\alpha_2\zeta_3^2-3\alpha_1^2\alpha_2\zeta_3^2-3\alpha_2^2\zeta_3^2 \\ & +3\alpha_1\alpha_2^2\zeta_3^2+24\alpha_1\zeta_3^3-6\alpha_1^2\zeta_3^3+18\alpha_2\zeta_3^3-6\alpha_1\alpha_2\zeta_3^3 \end{aligned} \quad (11.5)$$

$\zeta_3^2+\zeta_3+1$ による剰余を取り、 ζ_3 の次数を1以下に低減させる。

$$PQ = -18\alpha_1-9\alpha_1^2-3\alpha_1^3+18\alpha_2+3\alpha_1^2\alpha_2-36\alpha_1\zeta_3-6\alpha_1^3\zeta_3-18\alpha_2\zeta_3-3\alpha_1^2\alpha_2\zeta_3 \quad (11.6)$$

α_1^2+6 による剰余を取り、 α_1 の次数を1以下に低減させると、 $PQ=54$ となる。

(追記) 実はこの体は $f(x)=x^3+3x+2$ の分解体で、 $P=-9x, Q=3(x^2+3)$ である。よって、 $PQ=54$ となる。

つぎに、 $f(x)$ の分解体 F_s に属する2つの元を P, Q とし、商 P/Q を求める方法を示す。ただし、商は $\alpha_1, \alpha_2, \dots, \alpha_s$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_s}$ からなる分数式を多項式に書き換えて表すものとする。まず

$$P/Q = c_0 + c_1 \alpha_s + \dots + c_{p_s-1} \alpha_s^{p_s-1} \quad (c_0, c_1, \dots, c_{p_s-1} \text{は未知の係数}) \quad (11.7)$$

として、 $Q(c_0 + c_1 \alpha_s + \dots + c_{p_s-1} \alpha_s^{p_s-1}) - P = 0$ の左辺を展開し、 $\alpha_s^{p_s} - A_s$ による剰余を取り、 α_s の次数を p_s-1 以下に低減させる。そして、左辺の各係数が0となるように $c_0, c_1, \dots, c_{p_s-1}$ を決める。これを(11.7)に代入すれば、 P/Q は α_s の分数式から α_s の多項式に書き換えられる。つぎに、これを通分し、改めてその分子を P 、分母を Q とする。

$$P/Q = c_0 + c_1 \zeta_{p_s} + \dots + c_{p_s-2} \zeta_{p_s}^{p_s-2} \quad (c_0, c_1, \dots, c_{p_s-2} \text{は未知の係数}) \quad (11.8)$$

として、 $Q(c_0 + c_1 \zeta_{p_s} + \dots + c_{p_s-2} \zeta_{p_s}^{p_s-2}) - P = 0$ の左辺を展開し、 $\zeta_{p_s}^{p_s-1} + \dots + \zeta_{p_s} + 1$ による剰余を取り、 ζ_{p_s} の次数を p_s-2 以下に低減させる。そして、左辺の各係数が0となるように $c_0, c_1, \dots, c_{p_s-2}$ を決める。これを(11.8)に代入すれば、 P/Q は ζ_{p_s} の分数式から ζ_{p_s} の多項式に書き換えられる。同様に、 $\alpha_{s-1}, \zeta_{p_{s-1}}, \dots, \alpha_2, \zeta_{p_2}, \alpha_1, \zeta_{p_1}$ について分数式から多項式への書き換えを行う。

(例2) $s=2, p_1=2, p_2=3, \alpha_1^2+6=0, \alpha_2^3-3(1+\alpha_1+2\zeta_3)=0$ の場合

$P=54, Q=3-\alpha_2-\alpha_1\alpha_2+\alpha_2\zeta_3-\alpha_1\alpha_2\zeta_3-\alpha_2^2\zeta_3$ とし、商 P/Q を求める。まず、 $P/Q=c_0+c_1\alpha_2+c_2\alpha_2^2$ として、 c_0, c_1, c_2 を求める。 $Q(c_0+c_1\alpha_2+c_2\alpha_2^2)-P=0$ の左辺を展開し、 $\alpha_2^3-3(1+\alpha_1+2\zeta_3)$ による剰余を取り、 α_2 の次数を2以下に低減させれば次式となる。

$$\begin{aligned} & -54+3c_0-3(1+\alpha_1+2\zeta_3)\zeta_3c_1-3(1+\alpha_1+2\zeta_3)(1+\alpha_1-\zeta_3+\alpha_1\zeta_3)c_2 \\ & + \{- (1+\alpha_1-\zeta_3+\alpha_1\zeta_3)c_0+3c_1-3(1+\alpha_1+2\zeta_3)\zeta_3c_2\} \alpha_2 \\ & + \{-c_0\zeta_3-(1+\alpha_1-\zeta_3+\alpha_1\zeta_3)c_1+3c_2\} \alpha_2^2=0 \end{aligned} \quad (11.9)$$

これより、 c_0, c_1, c_2 は次式となる。

$$c_0=54(-3+\zeta_3+2\alpha_1\zeta_3+\alpha_1^2\zeta_3+\zeta_3^2+2\alpha_1\zeta_3^2+\alpha_1^2\zeta_3^2-2\zeta_3^3+2\alpha_1\zeta_3^3)/D \quad (11.10)$$

$$c_1=54(-1-\alpha_1+\zeta_3-\alpha_1\zeta_3-\zeta_3^2-\alpha_1\zeta_3^2-2\zeta_3^3)/D \quad (11.11)$$

$$c_2=18(-1-2\alpha_1-\alpha_1^2-\zeta_3-2\alpha_1^2\zeta_3-\zeta_3^2+2\alpha_1\zeta_3^2-\alpha_1^2\zeta_3^2)/D \quad (11.12)$$

$$\begin{aligned} D = & -8+4\alpha_1+6\alpha_1^2+4\alpha_1^3+\alpha_1^4+8\zeta_3+18\alpha_1\zeta_3+15\alpha_1^2\zeta_3+8\alpha_1^3\zeta_3+3\alpha_1^4\zeta_3+6\zeta_3^2+12\alpha_1\zeta_3^2+9\alpha_1^2\zeta_3^2 \\ & +6\alpha_1^3\zeta_3^2+3\alpha_1^4\zeta_3^2-10\zeta_3^3+20\alpha_1\zeta_3^3-3\alpha_1^2\zeta_3^3+4\alpha_1^3\zeta_3^3+\alpha_1^4\zeta_3^3+10\zeta_3^4+18\alpha_1\zeta_3^4-6\alpha_1^2\zeta_3^4 \\ & +2\alpha_1^3\zeta_3^4+12\zeta_3^5 \end{aligned} \quad (11.13)$$

これを $P/Q=c_0+c_1\alpha_2+c_2\alpha_2^2$ に代入して通分すれば次式となる。

$$\begin{aligned} P/Q = & \{54(-3+\zeta_3+2\alpha_1\zeta_3+\alpha_1^2\zeta_3+\zeta_3^2+2\alpha_1\zeta_3^2+\alpha_1^2\zeta_3^2-2\zeta_3^3+2\alpha_1\zeta_3^3) \\ & +54(-1-\alpha_1+\zeta_3-\alpha_1\zeta_3-\zeta_3^2-\alpha_1\zeta_3^2-2\zeta_3^3)\alpha_2 \\ & +18(-1-2\alpha_1-\alpha_1^2-\zeta_3-2\alpha_1^2\zeta_3-\zeta_3^2+2\alpha_1\zeta_3^2-\alpha_1^2\zeta_3^2)\alpha_2^2\}/D \end{aligned} \quad (11.14)$$

右辺の分子を改めて P 、分母を改めて Q とする。つぎに、 $P/Q=c_0+c_1\zeta_3$ として、 c_0, c_1 を求める。

$Q(c_0+c_1\zeta_3)-P=0$ の左辺を展開し、 $\zeta_3^2+\zeta_3+1$ による剰余を取り、 ζ_3 の次数を1以下に低減させれば次式となる。

$$\begin{aligned} & 18(18+3\alpha_1^2+6\alpha_2+4\alpha_1\alpha_2^2)-(36-12\alpha_1+6\alpha_1^2-2\alpha_1^3+\alpha_1^4)c_0-4(6+\alpha_1^2)\alpha_1c_1 \\ & + \{-18(6-2\alpha_1\alpha_2-\alpha_1^2\alpha_2)\alpha_2+4(6+\alpha_1^2)\alpha_1c_0-(36+12\alpha_1+6\alpha_1^2+2\alpha_1^3+\alpha_1^4)c_1\}\zeta_3=0 \end{aligned} \quad (11.15)$$

これより、 c_0, c_1 は次式となる。

$$c_0=54(216+72\alpha_1+72\alpha_1^2+24\alpha_1^3+12\alpha_1^4+2\alpha_1^5+\alpha_1^6+72\alpha_2+72\alpha_1\alpha_2+12\alpha_1^2\alpha_2+12\alpha_1^3\alpha_2+2\alpha_1^4\alpha_2+48\alpha_1\alpha_2^2)/D \quad (11.16)$$

$$c_1=18(432\alpha_1+144\alpha_1^3+12\alpha_1^5-216\alpha_2+216\alpha_1\alpha_2-36\alpha_1^2\alpha_2+36\alpha_1^3\alpha_2-6\alpha_1^4\alpha_2+72\alpha_1\alpha_2^2+108\alpha_1^2\alpha_2^2+18\alpha_1^4\alpha_2^2+\alpha_1^6\alpha_2^2)/D \quad (11.17)$$

$$D=1296+864\alpha_1^2+252\alpha_1^4+24\alpha_1^6+\alpha_1^8 \quad (11.18)$$

これを $P/Q=c_0+c_1\zeta_3$ に代入して通分すれば次式となる。

$$\begin{aligned} P/Q = \{ & 54(216+72\alpha_1+72\alpha_1^2+24\alpha_1^3+12\alpha_1^4+2\alpha_1^5+\alpha_1^6+72\alpha_2+72\alpha_1\alpha_2+12\alpha_1^2\alpha_2+12\alpha_1^3\alpha_2 \\ & +2\alpha_1^4\alpha_2+48\alpha_1\alpha_2^2)+18(432\alpha_1+144\alpha_1^3+12\alpha_1^5-216\alpha_2+216\alpha_1\alpha_2-36\alpha_1^2\alpha_2+36\alpha_1^3\alpha_2 \\ & -6\alpha_1^4\alpha_2+72\alpha_1\alpha_2^2+108\alpha_1^2\alpha_2^2+18\alpha_1^4\alpha_2^2+\alpha_1^6\alpha_2^2)\zeta_3\} / D \end{aligned} \quad (11.19)$$

右辺の分子を改めて P 、分母を改めて Q とする。つぎに、 $P/Q=c_0+c_1\alpha_1$ として、 c_0, c_1 を求める。

$Q(c_0+c_1\alpha_1)-P=0$ の左辺を展開し、 α_1^2+6 による剰余を取り、 α_1 の次数を1以下に低減させれば次式となる。

$$-3888\alpha_2(1-\zeta_3-\alpha_2\zeta_3)+1296c_0+1296\{-\alpha_2^2(2+\zeta_3)+c_1\}\alpha_1=0 \quad (11.20)$$

これより、 c_0, c_1 は次式となる。

$$c_0=3\alpha_2(1-\zeta_3-\alpha_2\zeta_3), \quad c_1=\alpha_2^2(2+\zeta_3) \quad (11.21)$$

これを $P/Q=c_0+c_1\alpha_1$ に代入すれば次式となる。

$$P/Q=3\alpha_2+2\alpha_1\alpha_2^2-3\alpha_2\zeta_3-3\alpha_2^2\zeta_3+\alpha_1\alpha_2^2\zeta_3 \quad (11.22)$$

数式処理ソフトによる計算

《サブプログラム》

alpha[1], alpha[2], ..., alpha[s]の多項式の次数を低減する。

(* Reduction of alpha[1], alpha[2], ..., alpha[s] *)

```
ReductionOfAlpha[f_] := Module[{a, b, g, i},
  g = f;
  For[i = Length[ListOfAlpha], i >= 1, i--,
    a = Part[ListOfAlpha, i, 1];
    b = Part[ListOfAlpha, i, 2];
    g = PolynomialRemainder[g, b, a];
  ];
  Return[Expand[Simplify[g]]];
];
```

ここで、ListOfAlphaには体の拡大で付加された $\zeta_{p_1}, \alpha_1, \zeta_{p_2}, \alpha_2, \dots, \zeta_{p_s}, \alpha_s$ とその条件式(11.3), (11.2)を前もって代入しておく。

```
ListOfAlpha = {{\zeta_{p_1}, \zeta_{p_1}^{p_1-1} + \dots + \zeta_{p_1} + 1}, {\alpha_1, \alpha_1^{p_1} - A_1},
  {\zeta_{p_2}, \zeta_{p_2}^{p_2-1} + \dots + \zeta_{p_2} + 1}, {\alpha_2, \alpha_2^{p_2} - A_2}, \dots, {\zeta_{p_s}, \zeta_{p_s}^{p_s-1} + \dots + \zeta_{p_s} + 1}, {\alpha_s, \alpha_s^{p_s} - A_s}};
```

《サブプログラム(2)》

分数式を多項式に書き換える。

(* Transform Fraction into Polynomial *)

```
FracToPoly[f_] := Module[{a, b, c, e, eqns, g, i, j, PQ, sol},
  g = f;
  For[i = Length[ListOfAlpha], i >= 1, i--,
    a = Part[ListOfAlpha, i, 1];
    b = Part[ListOfAlpha, i, 2];
    e = Exponent[b, a];
    PQ = Sum[c[j] * a^j, {j, 0, e-1}];
    eqns = PolynomialRemainder[Numerator[Together[Expand[g-PQ]]], b, a];
    sol = Solve[Table[Coefficient[eqns, a, j] == 0, {j, 0, e-1}], Table[c[j], {j, 0, e-1}]]];
```

```

g=ReplaceAll[PQ, Part[sol, 1]]
];
Return[Expand[Simplify[g]]]
];

```

ここで

Numerator[f] : 分数式fの分子を取り出す。

Together[f] : 分数式fを通分する。

sol=Solve[eqns, vars] : 方程式(または連立方程式)eqnsを解き, 未知数varsを求める。

その解vars(一般には複数通りの解がある)を配列solに代入する。

ReplaceAll[PQ, Part[sol, 1]] : PQにsol(上記の方程式の解)の第1解を代入する。

《メインプログラム》

```

ListOfAlpha={ {alpha[1], alpha[1]^2+6}, {z[3], z[3]^2+z[3]+1},
  {alpha[2], alpha[2]^3-3*(1+alpha[1]+2*z[3])} };
P=3*alpha[2]+2*alpha[1]*alpha[2]^2-3*alpha[2]*z[3]-3*alpha[2]^2*z[3]+
  alpha[1]*alpha[2]^2*z[3];
Q=3-alpha[2]-alpha[1]*alpha[2]+alpha[2]*z[3]-alpha[1]*alpha[2]*z[3]-
  alpha[2]^2*z[3];
Print["P=", P];
Print["Q=", Q];
Print["P*Q=", ReductionOfAlpha[P*Q]];
P=54;
Print["P=", P];
Print["Q=", Q];
Print["P/Q=", FracToPoly[P/Q]];

```

《計算結果》

```

P=3alpha[2]+2alpha[1]alpha[2]^2-3alpha[2]z[3]-3alpha[2]^2z[3]+
  alpha[1]alpha[2]^2z[3]
Q=3-alpha[2]-alpha[1]alpha[2]+alpha[2]z[3]-alpha[1]alpha[2]z[3]-alpha[2]^2z[3]
P*Q=54
P=54
Q=3-alpha[2]-alpha[1]alpha[2]+alpha[2]z[3]-alpha[1]alpha[2]z[3]-alpha[2]^2z[3]
P/Q=3alpha[2]+2alpha[1]alpha[2]^2-3alpha[2]z[3]-3alpha[2]^2z[3]+
  alpha[1]alpha[2]^2z[3]

```

12. 体の拡大と $g(x)$ の次数低減

先に求めた $g(x)$ は体 F_0 における v の最小多項式である。これに続いて、体 $F_1, F_2, \dots, F_s$ における v の最小多項式 $g_1(x), g_2(x), \dots, g_s(x)$ を求める。体 F_k における v の最小多項式 $g_k(x)$ ($k=1, 2, \dots, s$)は、 $x-v$ を G_k のすべての元で置換したものの積として次式で与える。

$$g_k(x) = \prod_{\sigma_i \in G_k} \sigma_i(x-v) = \prod_{\sigma_i \in G_k} (x-v_i) \quad (12.1)$$

このとき、 v_i は v の多項式で表されるから、 $g_k(x)$ の係数は v の多項式であって、 $g_k(x)$ は体 F_k 上の多項式にはなっていない。これを以下のようにして、体 F_k 上の多項式に書き換える。まず、 $k=0$ の場合は、 $g(x)$ は既に体 F_0 上の多項式になっている。つぎに、 $k \geq 1$ の場合は、 $g_{k-1}(x)$ が体 F_{k-1} 上の多項式であるとして、以下のようにして、 $g_k(x)$ を体 F_k 上の多項式に書き換える。まず、 G_{k-1} に属していて G_k に属していない任意の1つの置換を σ とし、 $g_k(x)$ を $\sigma^0, \sigma^1, \dots, \sigma^{p_k-1}$ で置換したものを $h_0(x), h_1(x), \dots, h_{p_k-1}(x)$ とする。つぎに、 $\theta_i(x)$ ($i=0, 1, \dots, p_k-1$)を次式で定める。

$$\theta_i(x) = (1/p_k) \{h_0(x) + \zeta_{p_k}^i h_1(x) + \dots + \zeta_{p_k}^{i(p_k-1)} h_{p_k-1}(x)\} \quad (i=0, 1, \dots, p_k-1) \quad (12.2)$$

ここで、体 F_{k-1} に ζ_{p_k} を付加した体を $\hat{F}_{k-1}$ とする。このとき、以下の①～③が成り立つ。

①置換 σ によって、 $h_0(x)$ は $h_1(x)$ に、 $h_1(x)$ は $h_2(x)$ に、そして $h_{p_k-1}(x)$ は $h_0(x)$ に移る。

②置換 σ によって、 $\theta_i(x)$ ($i=0, 1, \dots, p_k-1$)は $\zeta_{p_k}^{-i} \theta_i(x)$ に変わる。

③置換 σ によって、 $\{\theta_i(x)\}^{p_k}$ ($i=1, 2, \dots, p_k-1$)は変わらない。

これより、以下のようにして、 $\theta_i(x)$ ($i=0, 1, \dots, p_k-1$)を体 F_k 上の多項式として求める。

(1) (12.2)より $\theta_0(x)$ を求める。 $\theta_0(x)$ の係数はこの時点では v の多項式であるが、上記②によると置換 σ によって変わらないから、体 $\hat{F}_{k-1}$ の元に書き換えられるはずである。各係数について $g_{k-1}(v)$ による剰余を取ると、定数項(v^0 の項)だけが残って、これが体 $\hat{F}_{k-1}$ の元—— $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_k}$ の多項式で表される。——となる。このようにして、 $\theta_0(x)$ の係数は体 $\hat{F}_{k-1}$ の元に書き換えられる。

(2) (12.2)より $\{\theta_i(x)\}^{p_k}$ の最高次係数 A_i ($i=1, 2, \dots, p_k-1$)を求める。上記③によるとこれらは置換 σ によって変わらないから、 $\theta_0(x)$ の係数と同様にして、体 $\hat{F}_{k-1}$ の元に書き換えられる。ここでは最高次係数 A_i 以外は求める必要がない。

(3) A_i を $i=1, 2, \dots, p_k-1$ の順に見て行って、最初に $A_i \neq 0$ となったときを $i=m$ とする。ここで、体 $\hat{F}_{k-1}$ を体 F_k に拡大するために付加するべき根を $\alpha_k = \sqrt[p_k]{A_m}$ と定める。

(4) (12.2)より $\theta_m(x)$ の最高次係数 a_m を求める。これは体 $\hat{F}_{k-1}$ の元ではないから、 v の多項式として残しておく。

(5) (12.2)より $\theta_i(x)$ ($i=m, m+1, \dots, p_k-1$)を求める。これは体 $\hat{F}_{k-1}$ 上の多項式ではないから、各係数は v の多項式として残しておく。

(6) 次式より $\eta_i(x)$ ($i=m, m+1, \dots, p_k-1$)を求める。

$$\eta_i(x) = a_m^{p_k-j} \theta_i(x) \quad (12.3)$$

ここで、右辺の j は $jm=i$ (p_k を法とする)、 $1 \leq j \leq p_k-1$ を満たす整数とする。 $\eta_i(x)$ の係数はこの時点では v の多項式であるが、以下に示すように、体 $\hat{F}_{k-1}$ の元に書き換えられる。

(証明) $\eta_i(x)$ は置換 σ によって変わらないことを示せばよい。 a_m は $\theta_m(x)$ の最高次係数であるから、置換 σ によって $\zeta_{p_k}^{-m} a_m$ に変わる。 $\theta_i(x)$ は置換 σ によって $\zeta_{p_k}^{-i} \theta_i(x)$ に変わる。これより、 $\eta_i(x)$ は置換 σ によって以下のように変わる。

$$(\zeta_{p_k}^{-m} a_m)^{p_k-j} \zeta_{p_k}^{-i} \theta_i(x) = \zeta_{p_k}^{jm-i-mp_k} a_m^{p_k-j} \theta_i(x) = a_m^{p_k-j} \theta_i(x) = \eta_i(x) \quad (12.4)$$

$\eta_i(x)$ は置換 σ によって変わらないから、 $\eta_i(x)$ は体 $\hat{F}_{k-1}$ 上の多項式となる。(証明終わり)

そして、(12.3) より求めた $\eta_i(x)$ について、各係数を v の多項式から体 $\hat{F}_{k-1}$ の元書き換える。

(7) 次式より $\theta_i(x)$ ($i=m, m+1, \dots, p_k-1$) を体 F_k 上の多項式として求める。

$$\theta_i(x) = a_m^j \{ \eta_i(x) / a_m^{p_k} \} = \alpha_k^j \{ \eta_i(x) / A_m \} \quad (12.5)$$

ここで、 α_k は上記(3)で定めたべき根で、第11節で述べたように、文字のままで扱うことにする。
商 $\eta_i(x) / A_m$ は第11節で述べた方法によって、分数式から多項式に書き換える。

以上のようにして、 $\theta_i(x)$ ($i=0, 1, \dots, p_k-1$) が体 F_k 上の多項式として求められる。最後に、 $g_k(x) = h_0(x)$ は次式で求められる。

$$g_k(x) = \theta_0(x) + \theta_1(x) + \dots + \theta_{p_k-1}(x) \quad (12.6)$$

(例4) $f(x) = x^4 + 2x^3 + 3x^2 + 4x + 5$ の場合

第10節の(例4)の計算結果を使う。(10.22)の右辺に(10.28)の置換を作用させたものを $v_1, v_2, \dots, v_{24}$ とする。これに(10.24)–(10.27)を代入することにより、 $v_1, v_2, \dots, v_{24}$ を v の多項式として表す。そして、(10.29)の部分群 G_1, G_2, G_3, G_4 に対応して、拡大体 F_1, F_2, F_3, F_4 と最小多項式 $g_1(x), g_2(x), g_3(x), g_4(x)$ を求める。

《第1段階》

体 F_1 と最小多項式 $g_1(x)$ を求める。この場合は $p_1 = |G_0/G_1| = 2$ である。 $\sigma = \sigma_2$ とすれば、 $h_0(x), h_1(x)$ は次式となる。

$$h_0(x) = (x-v_1)(x-v_4)(x-v_5)(x-v_8)(x-v_9)(x-v_{12})(x-v_{13})(x-v_{16})(x-v_{17})(x-v_{20}) \\ \times (x-v_{21})(x-v_{24}) \quad (12.7)$$

$$h_1(x) = (x-v_2)(x-v_3)(x-v_6)(x-v_7)(x-v_{10})(x-v_{11})(x-v_{14})(x-v_{15})(x-v_{18})(x-v_{19}) \\ \times (x-v_{22})(x-v_{23}) \quad (12.8)$$

(12.2) より、 $\theta_0(x), \theta_1(x)$ は次式となる。

$$\theta_0(x) = (1/2) \{ h_0(x) + h_1(x) \} \quad (12.9)$$

$$\theta_1(x) = (1/2) \{ h_0(x) - h_1(x) \} \quad (12.10)$$

あとは前述の手順のとおり計算していく。

(1) $\theta_0(x)$ を体 $\hat{F}_0$ 上の多項式として求める。

$$\theta_0(x) = x^{12} + 12x^{11} + 96x^{10} + 520x^9 + 2022x^8 + 5808x^7 + 11420x^6 + 13704x^5 + 35793x^4 + 110564x^3 \\ + 396300x^2 + 575760x + 1352400 \quad (12.11)$$

(2) 最高次係数 A_1 を体 $\hat{F}_0$ の元として求める。

$$A_1 = 38880000 \quad (12.12)$$

(3) $A_1 \neq 0$ より $m=1$ とする。ここで付加するべき根は $\alpha_1 = \sqrt{A_1}$ と定める。これより

$$\alpha_1^2 - 38880000 = 0 \quad (12.13)$$

(4) 最高次係数 a_m を v の多項式として求める。ただし、計算結果は長いので省略する。

(5) $\theta_1(x)$ の係数を v の多項式として求める。ただし、計算結果は長いので省略する。

(6) $\eta_1(x)$ を体 $\hat{F}_0$ 上の多項式として求める。

$$\eta_1(x) = 38880000x^6 + 233280000x^5 + 933120000x^4 + 2177280000x^3 + 256608000x^2 - 3219264000x - 637632000 \quad (12.14)$$

(7) $\theta_1(x)$ を体 F_1 上の多項式として求める。

$$\theta_1(x) = \alpha_1 \{x^6 + 6x^5 + 24x^4 + 56x^3 + (33/5)x^2 - (414/5)x - 82/5\} \quad (12.15)$$

最後に, (12.6) より体 F_1 における v の最小多項式 $g_1(x)$ を求める。

$$\begin{aligned} g_1(x) = & x^{12} + 12x^{11} + 96x^{10} + 520x^9 + 2022x^8 + 5808x^7 + (11420 + \alpha_1)x^6 + (13704 + 6\alpha_1)x^5 \\ & + (35793 + 24\alpha_1)x^4 + (110564 + 56\alpha_1)x^3 + \{396300 + (33/5)\alpha_1\}x^2 \\ & + \{575760 - (414/5)\alpha_1\}x + \{1352400 - (82/5)\alpha_1\} \end{aligned} \quad (12.16)$$

《第2段階》

体 F_2 と最小多項式 $g_2(x)$ を求める。この場合は $p_2 = |G_1/G_2| = 3$ である。 $\sigma = \sigma_4$, $\sigma^2 = \sigma_5$ とすれば, $h_0(x)$, $h_1(x)$, $h_2(x)$ は次式となる。

$$h_0(x) = (x-v_1)(x-v_8)(x-v_{17})(x-v_{24}) \quad (12.17)$$

$$h_1(x) = (x-v_4)(x-v_{12})(x-v_{13})(x-v_{21}) \quad (12.18)$$

$$h_2(x) = (x-v_5)(x-v_9)(x-v_{16})(x-v_{20}) \quad (12.19)$$

(12.2) より, $\theta_0(x)$, $\theta_1(x)$, $\theta_2(x)$ は次式となる。

$$\theta_0(x) = (1/3) \{h_0(x) + h_1(x) + h_2(x)\} \quad (12.20)$$

$$\theta_1(x) = (1/3) \{h_0(x) + \zeta_3 h_1(x) + \zeta_3^2 h_2(x)\} \quad (12.21)$$

$$\theta_2(x) = (1/3) \{h_0(x) + \zeta_3^2 h_1(x) + \zeta_3 h_2(x)\} \quad (12.22)$$

ここで

$$\zeta_3^2 + \zeta_3 + 1 = 0 \quad (12.23)$$

あとは前述の手順のとおりに計算していく。

(1) $\theta_0(x)$ を体 $\hat{F}_1$ 上の多項式として求める。

$$\theta_0(x) = x^4 + 4x^3 + 16x^2 + 24x + 230 \quad (12.24)$$

(2) 最高次係数 A_1, A_2 を体 $\hat{F}_1$ の元として求める。

$$A_1 = 2120 + (19/135)\alpha_1 + 1440\zeta_3 - (14/27)\alpha_1\zeta_3 \quad (12.25)$$

$$A_2 = 680 + (89/135)\alpha_1 - 1440\zeta_3 + (14/27)\alpha_1\zeta_3 \quad (12.26)$$

(3) $A_1 \neq 0$ より $m=1$ とする。ここで付加するべき根は $\alpha_2 = \sqrt[3]{A_1}$ と定める。これより

$$\alpha_2^3 - \{2120 + (19/135)\alpha_1 + 1440\zeta_3 - (14/27)\alpha_1\zeta_3\} = 0 \quad (12.27)$$

(4) 最高次係数 a_m を v の多項式として求める。ただし, 計算結果は長いため省略する。

(5) $\theta_1(x)$, $\theta_2(x)$ の係数を v の多項式として求める。ただし, 計算結果は長いため省略する。

(6) $\eta_1(x)$, $\eta_2(x)$ を体 $\hat{F}_1$ 上の多項式として求める。

$$\begin{aligned} \eta_1(x) = & \{2120 + (19/135)\alpha_1 + 1440\zeta_3 - (14/27)\alpha_1\zeta_3\}x^2 \\ & + \{4240 + (38/135)\alpha_1 + 2880\zeta_3 - (28/27)\alpha_1\zeta_3\}x \\ & + 39860 - (62/135)\alpha_1 + 27840\zeta_3 - (412/135)\alpha_1\zeta_3 \end{aligned} \quad (12.28)$$

$$\eta_2(x) = 260x^2 + 520x + 2090 - (31/180)\alpha_1 + 360\zeta_3 - (5/18)\alpha_1\zeta_3 \quad (12.29)$$

(7) $\theta_1(x)$, $\theta_2(x)$ を体 F_2 上の多項式として求める。

$$\theta_1(x) = \alpha_2 \{x^2 + 2x + 173/26 + (19/46800)\alpha_1 - (18/13)\zeta_3 + (1/936)\alpha_1\zeta_3\} \quad (12.30)$$

$$\begin{aligned} \theta_2(x) = & \alpha_2^2 [\{17/1690 + (89/9126000)\alpha_1 - (18/845)\zeta_3 + (7/912600)\alpha_1\zeta_3\}x^2 \\ & + \{17/845 + (89/4563000)\alpha_1 - (36/845)\zeta_3 + (7/456300)\alpha_1\zeta_3\}x \\ & + 601/3380 + (7/182520)\alpha_1 - (348/845)\zeta_3 + (103/2281500)\alpha_1\zeta_3] \end{aligned} \quad (12.31)$$

最後に、(12.6)より体 F_2 における v の最小多項式 $g_2(x)$ を求める。

$$\begin{aligned} g_2(x) = & x^4 + 4x^3 + \{16 + \alpha_2 + (17/1690)\alpha_2^2 + (89/9126000)\alpha_1\alpha_2^2 - (18/845)\alpha_2^2\zeta_3 + (7/912600)\alpha_1\alpha_2^2\zeta_3\}x^2 \\ & + \{24 + 2\alpha_2 + (17/845)\alpha_2^2 + (89/4563000)\alpha_1\alpha_2^2 - (36/845)\alpha_2^2\zeta_3 + (7/456300)\alpha_1\alpha_2^2\zeta_3\}x \\ & + 230 + (173/26)\alpha_2 + (19/46800)\alpha_1\alpha_2 + (601/3380)\alpha_2^2 + (7/182520)\alpha_1\alpha_2^2 \\ & - (18/13)\alpha_2\zeta_3 + (601/3380)\alpha_1\alpha_2\zeta_3 - (348/845)\alpha_2^2\zeta_3 + (103/2281500)\alpha_1\alpha_2^2\zeta_3 \end{aligned} \quad (12.32)$$

《第3段階》

体 F_3 と最小多項式 $g_3(x)$ を求める。この場合は $p_3 = |G_2/G_3| = 2$ である。 $\sigma = \sigma_{17}$ とすれば、 $h_0(x), h_1(x)$ は次式となる。

$$h_0(x) = (x - v_1)(x - v_8) \quad (12.33)$$

$$h_1(x) = (x - v_{17})(x - v_{24}) \quad (12.34)$$

(12.2)より、 $\theta_0(x), \theta_1(x)$ は次式となる。

$$\theta_0(x) = (1/2)\{h_0(x) + h_1(x)\} \quad (12.35)$$

$$\theta_1(x) = (1/2)\{h_0(x) - h_1(x)\} \quad (12.36)$$

あとは前述の手順のとおりに計算していく。

(1) $\theta_0(x)$ を体 $\hat{F}_2$ 上の多項式として求める。

$$\begin{aligned} \theta_0(x) = & x^2 + 2x + 4 + (11/26)\alpha_2 + (47/3380)\alpha_2^2 + (29/6084000)\alpha_1\alpha_2^2 - (4/13)\alpha_2\zeta_3 \\ & - (1/169)\alpha_2^2\zeta_3 + (19/3042000)\alpha_1\alpha_2^2\zeta_3 \end{aligned} \quad (12.37)$$

(2) 最高次係数 A_1 を体 $\hat{F}_2$ の元として求める。

$$\begin{aligned} A_1 = & -4 - (2/13)\alpha_2 + (3/169)\alpha_2^2 - (1/4563000)\alpha_1\alpha_2^2 - (8/13)\alpha_2\zeta_3 + (8/845)\alpha_2^2\zeta_3 \\ & + (11/2281500)\alpha_1\alpha_2^2\zeta_3 \end{aligned} \quad (12.38)$$

(3) $A_1 \neq 0$ より $m=1$ とする。ここで付加するべき根は $\alpha_3 = \sqrt{A_1}$ と定める。これより

$$\begin{aligned} \alpha_3^2 - \{-4 - (2/13)\alpha_2 + (3/169)\alpha_2^2 - (1/4563000)\alpha_1\alpha_2^2 - (8/13)\alpha_2\zeta_3 + (8/845)\alpha_2^2\zeta_3 \\ + (11/2281500)\alpha_1\alpha_2^2\zeta_3\} = 0 \end{aligned} \quad (12.39)$$

(4) 最高次係数 a_m を v の多項式として求める。ただし、計算結果は長いので省略する。

(5) $\theta_1(x)$ の係数を v の多項式として求める。ただし、計算結果は長いので省略する。

(6) $\eta_1(x)$ を体 $\hat{F}_2$ 上の多項式として求める。

$$\begin{aligned} \eta_1(x) = & \{-4 - (2/13)\alpha_2 + (3/169)\alpha_2^2 - (1/4563000)\alpha_1\alpha_2^2 - (8/13)\alpha_2\zeta_3 + (8/845)\alpha_2^2\zeta_3 \\ & + (11/2281500)\alpha_1\alpha_2^2\zeta_3\}(x+1) \end{aligned} \quad (12.40)$$

(7) $\theta_1(x)$ を体 F_3 上の多項式として求める。

$$\theta_1(x) = \alpha_3(x+1) \quad (12.41)$$

最後に、(12.6)より体 F_3 における v の最小多項式 $g_3(x)$ を求める。

$$\begin{aligned} g_3(x) = & x^2 + (2 + \alpha_3)x + 4 + (11/26)\alpha_2 + (47/3380)\alpha_2^2 + (29/6084000)\alpha_1\alpha_2^2 + \alpha_3 \\ & - (4/13)\alpha_2\zeta_3 - (1/169)\alpha_2^2\zeta_3 + (19/3042000)\alpha_1\alpha_2^2\zeta_3 \end{aligned} \quad (12.42)$$

《第4段階》

体 F_4 と最小多項式 $g_4(x)$ を求める。この場合は $p_4 = |G_3/G_4| = 2$ である。 $\sigma = \sigma_8$ とすれば、 $h_0(x), h_1(x)$ は次式となる。

$$h_0(x) = x - v_1 \quad (12.43)$$

$$h_1(x) = x - v_8 \quad (12.44)$$

(12.2)より、 $\theta_0(x), \theta_1(x)$ は次式となる。

$$\theta_0(x) = (1/2)\{h_0(x) + h_1(x)\} \quad (12.45)$$

$$\theta_1(x) = (1/2)\{h_0(x) - h_1(x)\} \quad (12.46)$$

あとは前述の手順のとおりに計算していく。

(1) $\theta_0(x)$ を体 $\hat{F}_3$ 上の多項式として求める。

$$\theta_0(x) = x + 1 + (1/2)\alpha_3 \quad (12.47)$$

(2) 最高次係数 A_1 を体 $\hat{F}_3$ の元として求める。

$$\begin{aligned} A_1 = & -4 - (6/13)\alpha_2 - (8/845)\alpha_2^2 - (11/2281500)\alpha_1\alpha_2^2 + (2/13)\alpha_2\zeta_3 + (7/845)\alpha_2^2\zeta_3 \\ & - (23/4563000)\alpha_1\alpha_2^2\zeta_3 \end{aligned} \quad (12.48)$$

(3) $A_1 \neq 0$ より $m=1$ とする。ここで付加するべき根は $\alpha_4 = \sqrt{A_1}$ と定める。これより

$$\begin{aligned} \alpha_4^2 - \{-4 - (6/13)\alpha_2 - (8/845)\alpha_2^2 - (11/2281500)\alpha_1\alpha_2^2 + (2/13)\alpha_2\zeta_3 + (7/845)\alpha_2^2\zeta_3 \\ - (23/4563000)\alpha_1\alpha_2^2\zeta_3\} = 0 \end{aligned} \quad (12.49)$$

(4) 最高次係数 a_m を v の多項式として求める。

$$a_m = -v - 1 - (1/2)\alpha_3 \quad (12.50)$$

(5) $\theta_1(x)$ の係数を v の多項式として求める。

$$\theta_1(x) = -v - 1 - (1/2)\alpha_3 \quad (12.51)$$

(6) $\eta_1(x)$ を体 $\hat{F}_3$ 上の多項式として求める。

$$\begin{aligned} \eta_1(x) = & -4 - (6/13)\alpha_2 - (8/845)\alpha_2^2 - (11/2281500)\alpha_1\alpha_2^2 + (2/13)\alpha_2\zeta_3 + (7/845)\alpha_2^2\zeta_3 \\ & - (23/4563000)\alpha_1\alpha_2^2\zeta_3 \end{aligned} \quad (12.52)$$

(7) $\theta_1(x)$ を体 F_4 上の多項式として求める。

$$\theta_1(x) = \alpha_4 \quad (12.53)$$

最後に, (12.6) より体 F_4 における v の最小多項式 $g_4(x)$ を求める。

$$g_4(x) = x + 1 + (1/2)\alpha_3 + \alpha_4 \quad (12.54)$$

数式処理ソフトによる計算

《メインプログラム》

本節の(例4)の第2段階の計算を行う。準備として, ファイル example4.txt を用意し, これに第10節の(例4)の計算結果(10.22)–(10.29)を書き込んでおく。このために, 第10節のプログラムを実行し, 入力要求 "f(x)= " に対して "x^4+2*x^3+3*x^2+4*x+5" を, "Output file name: " に対して "example4.txt" を入力する。これでファイル example4.txt が作られる。さらに, 第1段階の計算結果として, gx に (12.16) の $g_1(x)$ を, ListOfAlpha に α_1 とその条件式(12.13)を代入しておく。

```
SetDirectory["C:\Users\Myname\Documents\Mathematica"];
Get["example4.txt"];
n=Exponent[fx, x];
nn=Length[G];
For[i=1, i<=nn, i++,
  V[i]=Simplify[Sum[m[j]*X[Part[G, i, j]], {j, 1, n}]]
];
gx=x^12+12*x^11+96*x^10+520*x^9+2022*x^8+5808*x^7+(11420+alpha[1])*x^6+
  (13704+6*alpha[1])*x^5+(35793+24*alpha[1])*x^4+(110564+56*alpha[1])*x^3+
  (396300+(33/5)*alpha[1])*x^2+(575760-(414/5)*alpha[1])*x+
  1352400-(82/5)*alpha[1];
ProductOfG[];
z[2]=-1;
ListOfAlpha={ {alpha[1], alpha[1]^2-38880000} };
step=2;
```

```

G=Part[Gs, step];
H=Part[Gs, step+1];
p=Length[G]/Length[H];
For[i=1, MemberQ[H, s=Part[G, i]], i++, ];
For[i=0, i<=p-1, i++,
  h[i]=1;
  For[j=1, j<=Length[H], j++,
    h[i]=ReductionOfAlpha[PolynomialRemainder[
      Expand[h[i]*(x-V[Part[H, j]]], ReplaceAll[ gx, x->v], v]]
  ];
  H=Table[Part[ListOfProduct, s, Part[H, j]], {j, 1, Length[H]}]
];
If[p!=2, AppendTo[ListOfAlpha, {z[p], Sum[z[p]^i, {i, 0, p-1}]}]];
theta[0]=ReductionOfAlpha[PolynomialRemainder[
  Sum[h[j], {j, 0, p-1}], ReplaceAll[ gx, x->v], v]/p];
M=0;
For[i=1, i<=p-1, i++,
  theta[i]=ReductionOfAlpha[PolynomialRemainder[
    Sum[z[p]^(i*j)*h[j], {j, 0, p-1}], ReplaceAll[ gx, x->v], v]/p];
  temp=ReductionOfAlpha[PolynomialRemainder[
    Expand[theta[i]^p], ReplaceAll[ gx, x->v], v]];
  If[Exponent[temp, x]<0, theta[i]=0;Continue[]];
  If[M==0,
    M=i;
    Am=Coefficient[temp, x, Exponent[temp, x]];
    am=Coefficient[theta[i], x, Exponent[theta[i], x]]
  ];
  For[j=1, Mod[j*M-i, p]!=0, j++, ];
  eta=ReductionOfAlpha[PolynomialRemainder[
    Expand[am^(p-j)*theta[i]], ReplaceAll[ gx, x->v], v]];
  theta[i]=alpha[step]^j*FracToPoly[eta/Am]
];
AppendTo[ListOfAlpha, {alpha[step], alpha[step]^p-Am}];
For[i=0, i<=p-1, i++,
  Print["theta", i, "(x)=", theta[i]]
];
gx=ReductionOfAlpha[Expand[Sum[theta[i], {i, 0, p-1}]]];
Print["g", step, "(x)=", gx];
Print["List of alpha : "];
For[i=1, i<=Length[ListOfAlpha], i++,
  Print[Part[ListOfAlpha, i]]
];

```

ここで

Get[file] : ファイルfileに書かれたプログラムを実行する。
 $gx = x^{12} + \dots - (82/5) * \alpha[1]$: gx に(12.16)の $g_1(x)$ を代入する。
 ListOfAlpha={...} : ListOfAlphaに α_1 とその条件式(12.13)を代入する。
 For[i=1, MemberQ[H, s=Part[G, i]], i++,] : Gに属していてHに属していないsを求める。
 H=Table[...] : s番目の置換とHに属する置換との積を改めてHとする。
 If[p!=2, AppendTo[...]] : ListOfAlphaに ζ_3 とその条件式(12.23)を追加する。
 AppendTo[ListOfAlpha, ...] : ListOfAlphaに α_2 とその条件式(12.27)を追加する。

(注意) SetDirectory中の"C:\Users...¥Mathematica"は, 実際にファイルを置く場所書き換える。

《計算結果》

```
theta0(x)=230+24x+16x2+4x3+x4
theta1(x)=alpha[2](173/26+2x+x2+19alpha[1]/46800-18z[3]/13+alpha[1]z[3]/936)
theta2(x)=alpha[2]2(601/3380+17x/845+17x2/1690+7alpha[1]/182520+
89x alpha[1]/4563000+89x2alpha[1]/9126000-348z[3]/845-36x z[3]/845-
18x2z[3]/845+103alpha[1]z[3]/2281500+7x alpha[1]z[3]/456300+
7x2alpha[1]z[3]/912600)
g2(x)=230+24x+16x2+4x3+x4+173alpha[2]/26+2x alpha[2]+x2alpha[2]+
19alpha[1]alpha[2]/46800+601alpha[2]2/3380+17x alpha[2]2/845+
17x2alpha[2]2/1690+7alpha[1]alpha[2]2/182520+89x alpha[1]alpha[2]2/4563000+
89x2alpha[1]alpha[2]2/9126000-18alpha[2]z[3]/13+alpha[1]alpha[2]z[3]/936-
348alpha[2]2z[3]/845-36x alpha[2]2z[3]/845-18x2alpha[2]2z[3]/845+
103alpha[1]alpha[2]2z[3]/2281500+7x alpha[1]alpha[2]2z[3]/456300+
7x2alpha[1]alpha[2]2z[3]/912600
List of alpha :
{alpha[1], -38880000+alpha[1]2}
{z[3], 1+z[3]+z[3]2}
{alpha[2], -2120-19alpha[1]/135+alpha[2]3-1440z[3]+14alpha[1]z[3]/27}
```

13. 根 $x_1, x_2, \dots, x_n$ の計算

前節で述べたように、 $g(x)$ の次数低減を $g_1(x), g_2(x), \dots, g_s(x)$ と進めていくと、最後の $g_s(x)$ は1次式となり、 v が求められる。根 $x_1, x_2, \dots, x_n$ は v の多項式で表されるので、この v を代入すれば根 $x_1, x_2, \dots, x_n$ が求まる。ただし、実際には $x_1, x_2, \dots, x_n$ に v を直接代入するよりも、 $x_1, x_2, \dots, x_n$ について順次 $g_1(v), g_2(v), \dots, g_s(v)$ による剰余を取り、 v の次数を段階的に低減させていくほうが、計算するのは容易である。このようにして、根 $x_1, x_2, \dots, x_n$ が $\alpha_1, \alpha_2, \dots, \alpha_s$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_s}$ の多項式として求められる。そして、第11節で述べたように、 $\alpha_s, \zeta_{p_s}, \dots, \alpha_2, \zeta_{p_2}, \alpha_1, \zeta_{p_1}$ の順序で、(11.2)または(11.3)による剰余を取ることににより、 $\alpha_1, \alpha_2, \dots, \alpha_s$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_s}$ の次数を低減させる。

(例4) $f(x)=x^4+2x^3+3x^2+4x+5$ の場合

(10.24)–(10.27)で示した x_1, x_2, x_3, x_4 について、(12.16), (12.32), (12.42), (12.54)で示した $g_1(v), g_2(v), g_3(v), g_4(v)$ による剰余を取る。そして、(12.49), (12.39), (12.27), (12.23), (12.13)より $\alpha_4, \alpha_3, \alpha_2, \zeta_3, \alpha_1$ の次数を低減させる。これより、 x_1, x_2, x_3, x_4 は次式となる。

$$\begin{aligned} x_1 = & -1/2 + (1/4)\alpha_3 - (1/4)\alpha_4 - (1/16)\alpha_3\alpha_4 + (1/104)\alpha_2\alpha_3\alpha_4 - (7/54080)\alpha_2^2\alpha_3\alpha_4 \\ & + (23/292032000)\alpha_1\alpha_2^2\alpha_3\alpha_4 + (3/416)\alpha_2\alpha_3\alpha_4\zeta_3 - (3/10816)\alpha_2^2\alpha_3\alpha_4\zeta_3 \\ & + (1/292032000)\alpha_1\alpha_2^2\alpha_3\alpha_4\zeta_3 \end{aligned} \quad (13.1)$$

$$\begin{aligned} x_2 = & -1/2 + (1/4)\alpha_3 + (1/4)\alpha_4 + (1/16)\alpha_3\alpha_4 - (1/104)\alpha_2\alpha_3\alpha_4 + (7/54080)\alpha_2^2\alpha_3\alpha_4 \\ & - (23/292032000)\alpha_1\alpha_2^2\alpha_3\alpha_4 - (3/416)\alpha_2\alpha_3\alpha_4\zeta_3 + (3/10816)\alpha_2^2\alpha_3\alpha_4\zeta_3 \\ & - (1/292032000)\alpha_1\alpha_2^2\alpha_3\alpha_4\zeta_3 \end{aligned} \quad (13.2)$$

$$\begin{aligned} x_3 = & -1/2 - (1/4)\alpha_3 - (1/4)\alpha_4 + (1/16)\alpha_3\alpha_4 - (1/104)\alpha_2\alpha_3\alpha_4 + (7/54080)\alpha_2^2\alpha_3\alpha_4 \\ & - (23/292032000)\alpha_1\alpha_2^2\alpha_3\alpha_4 - (3/416)\alpha_2\alpha_3\alpha_4\zeta_3 + (3/10816)\alpha_2^2\alpha_3\alpha_4\zeta_3 \\ & - (1/292032000)\alpha_1\alpha_2^2\alpha_3\alpha_4\zeta_3 \end{aligned} \quad (13.3)$$

$$\begin{aligned} x_4 = & -1/2 - (1/4)\alpha_3 + (1/4)\alpha_4 - (1/16)\alpha_3\alpha_4 + (1/104)\alpha_2\alpha_3\alpha_4 - (7/54080)\alpha_2^2\alpha_3\alpha_4 \\ & + (23/292032000)\alpha_1\alpha_2^2\alpha_3\alpha_4 + (3/416)\alpha_2\alpha_3\alpha_4\zeta_3 - (3/10816)\alpha_2^2\alpha_3\alpha_4\zeta_3 \\ & + (1/292032000)\alpha_1\alpha_2^2\alpha_3\alpha_4\zeta_3 \end{aligned} \quad (13.4)$$

検算をするには、 $(x-x_1)(x-x_2)\dots(x-x_n)$ を展開して、各係数を $\alpha_1, \alpha_2, \dots, \alpha_s$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_s}$ の多項式として求め、(11.2)または(11.3)による剰余を取り、 $\alpha_1, \alpha_2, \dots, \alpha_s$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_s}$ の次数を低減させる。これが $f(x)$ と一致することを確認すればよい。ただし、実際には $(x-x_1)(x-x_2)\dots(x-x_n)$ を展開して $\alpha_1, \alpha_2, \dots, \alpha_s$ と $\zeta_{p_1}, \zeta_{p_2}, \dots, \zeta_{p_s}$ の次数を一挙に低減させるよりも、まず $(x-x_1)(x-x_2)$ を展開して次数を低減させ、これに $x-x_3$ を掛けて展開して次数を低減させ、同様にして、最後は $x-x_n$ を掛けて展開して次数を低減させるほうが、計算するのは容易である。

(例4) $f(x)=x^4+2x^3+3x^2+4x+5$ の場合

$(x-x_1)(x-x_2)(x-x_3)(x-x_4)$ に(13.1)–(13.4)を代入して展開し、(12.49), (12.39), (12.27), (12.23), (12.13)より $\alpha_4, \alpha_3, \alpha_2, \zeta_3, \alpha_1$ の次数を低減させる。まず $(x-x_1)(x-x_2)$ を展開して次数を低減させ、これに $x-x_3$ を掛けて展開して次数を低減させ、さらに $x-x_4$ を掛けて展開して次数を低減させる。これより、 $x^4+2x^3+3x^2+4x+5$ と一致することが確認できる。

近似値での検算も示す。まず, (12. 13), (12. 23) より α_1, ζ_3 は各々以下の2つの値を取る。

$$\alpha_1 = 6235.38, -6235.38 \quad (13.5)$$

$$\zeta_3 = -0.5 + 0.866025i, -0.5 - 0.866025i \quad (13.6)$$

第1の α_1 , 第1の ζ_3 を選ぶと, (12. 27) は $\alpha_2^3 - 3894.15 + 1552.92i = 0$ となる。これより, α_2 は以下の3つの値を取る。

$$\alpha_2 = 15.9957 - 2.03409i, -6.23628 + 14.8697i, -9.75942 - 12.8356i \quad (13.7)$$

第1の α_2 を選ぶと, (12. 39) は $\alpha_3^2 + 1.24633 = 0$ となる。これより, α_3 は以下の2つの値を取る。

$$\alpha_3 = 1.11639i, -1.11639i \quad (13.8)$$

第1の α_3 を選ぶと, (12. 49) は $\alpha_4^2 + 20.6841 = 0$ となる。これより, α_4 は以下の2つの値を取る。

$$\alpha_4 = 4.54798i, -4.54798i \quad (13.9)$$

第1の α_4 を選び, 以上の $\alpha_1, \zeta_3, \alpha_2, \alpha_3, \alpha_4$ を (13. 1) - (13. 4) に代入すると, 以下の x_1, x_2, x_3, x_4 が得られる。

$$\begin{aligned} x_1 &= -1.28782 - 0.857897i, \quad x_2 = 0.287815 + 1.41609i, \quad x_3 = 0.287815 - 1.41609i \\ x_4 &= -1.28782 + 0.857897i \end{aligned} \quad (13.10)$$

これは数値解法の結果と一致する。(12. 13), (12. 23), (12. 27), (12. 39), (12. 49) を満たす他の $\alpha_1, \zeta_3, \alpha_2, \alpha_3, \alpha_4$ ($2 \times 2 \times 3 \times 2 \times 2 = 48$ 通り) についても, x_1, x_2, x_3, x_4 の順序が入れ替わるだけで, すべて同じ結果となる。

14. 数式処理ソフトによる計算

第2部で示したプログラムを1つにまとめて、計算結果をファイルに書き込むようにした。

《サブプログラム》

$(x-X[1])(x-X[2])\cdots(x-X[n])$ を展開する。

```
(* Verification of X[1],X[2],...,X[n] *)
VerificationOfX[]:=Module[{i,LeftSide,RightSide},
  LeftSide="";
  For[i=1,i<=n,i++,
    LeftSide=StringJoin[LeftSide,"(x-X["ToString[i],"])"
  ];
  RightSide=1;
  For[i=1,i<=n,i++,
    RightSide=ReductionOfAlpha[Expand[RightSide*(x-X[i])]]
  ];
  Print[LeftSide,"=",RightSide]
];
```

ここで

StringJoin[s1,s2,...] : 文字列s1,s2,...を結合する。
ToString[f] : 数式fを文字列に変換する。

《サブプログラム(2)》

計算結果をファイルに書き込む。

```
(* Write Results into File *)
WriteFile2[FileName_] := Module[{fp, i},
  fp = OpenWrite[FileName];
  WriteString[fp, "fx=", InputForm[fx], ";¥n"];
  WriteString[fp, "ListOfAlpha=", InputForm[ListOfAlpha], ";¥n"];
  For[i=1,i<=n,i++,
    WriteString[fp, "X[" i, "]=", InputForm[X[i]], ";¥n"]
  ];
  Close[fp]
];
```

《メインプログラム》

```
(* Calculation of X[1],X[2],...,X[n] *)
SetDirectory["C:¥Users¥Myname¥Documents¥Mathematica"];
FileName=InputString["Input file name : "];
Get[FileName];
n=Exponent[fx,x];
nn=Length[G];
For[i=1,i<=nn,i++,
  V[i]=Simplify[Sum[m[j]*X[Part[G,i,j]],{j,1,n}]]
```

```

];
ProductOfG[];
z[2]=-1;
ListOfAlpha={};
For[step=1, step<Length[Gs], step++,
  Print["..... step ", step, " ....."];
  G=Part[Gs, step];
  H=Part[Gs, step+1];
  p=Length[G]/Length[H];
  For[i=1, MemberQ[H, s=Part[G, i]], i++, ];
  For[i=0, i<=p-1, i++,
    h[i]=1;
    For[j=1, j<=Length[H], j++,
      h[i]=ReductionOfAlpha[PolynomialRemainder[
        Expand[h[i]*(x-V[Part[H, j]]], ReplaceAll[ gx, x->v], v]]
    ];
    H=Table[Part[ListOfProduct, s, Part[H, j]], {j, 1, Length[H]}]
  ];
  If[p!=2, AppendTo[ListOfAlpha, {z[p], Sum[z[p]^i, {i, 0, p-1}]}]];
  theta[0]=ReductionOfAlpha[PolynomialRemainder[
    Sum[h[j], {j, 0, p-1}], ReplaceAll[ gx, x->v], v]/p];
  M=0;
  For[i=1, i<=p-1, i++,
    theta[i]=ReductionOfAlpha[PolynomialRemainder[
      Sum[z[p]^(i*j)*h[j], {j, 0, p-1}], ReplaceAll[ gx, x->v], v]/p];
    temp=ReductionOfAlpha[PolynomialRemainder[
      Expand[theta[i]^p], ReplaceAll[ gx, x->v], v]];
    If[Exponent[temp, x]<0, theta[i]=0;Continue[]];
    If[M==0,
      M=i;
      Am=Coefficient[temp, x, Exponent[temp, x]];
      am=Coefficient[theta[i], x, Exponent[theta[i], x]]
    ];
    For[j=1, Mod[j*M-i, p]!=0, j++, ];
    eta=ReductionOfAlpha[PolynomialRemainder[
      Expand[am^(p-j)*theta[i]], ReplaceAll[ gx, x->v], v]];
    theta[i]=alpha[step]^j*FracToPoly[eta/Am]
  ];
  AppendTo[ListOfAlpha, {alpha[step], alpha[step]^p-Am}];
  For[i=0, i<=p-1, i++,
    Print["theta", i, "(x)=", theta[i]]
  ];
  gx=ReductionOfAlpha[Expand[Sum[theta[i], {i, 0, p-1}]]];
  Print["g", step, "(x)=", gx];

```

```

For[i=1, i<=n, i++,
  X[i]=ReductionOfAlpha[PolynomialRemainder[X[i], ReplaceAll[gx, x->v], v]]
]
];
Print["List of alpha : "];
For[i=1, i<=Length[ListOfAlpha], i++,
  Print[Part[ListOfAlpha, i]]
];
For[i=1, i<=n, i++,
  Print["X[" , i, "]=", X[i]]
];
VerificationOfX[];
FileName=InputString["Output file name : "];
WriteFile2[FileName];

```

(注意) SetDirectory中の"C:\Users...¥Mathematica"は、実際にファイルを置く場所書き換える。

《計算結果》

$f(x)=x^3+a_2x^2+a_1x+a_0$ の計算結果を示す。準備として、ファイルexample1.txtを用意し、これに第10節の(例1)の計算結果(10.1)–(10.8)を書き込んでおく。このために、第10節のプログラムを実行し、入力要求"f(x)="に対して" $x^3+a_2x^2+a_1x+a_0$ "を、"Output file name : "に対して"example1.txt"を入力する。これでファイルexample1.txtが作られる。続いて本節のプログラムを実行し、入力要求"Input file name : "に対して"example1.txt"を入力する。

```

..... step 1 .....
theta0(x)=3a1 x-a2^2x+x^3
theta1(x)=alpha[1]
g1(x)=3a1 x-a2^2x+x^3+alpha[1]
..... step 2 .....
theta0(x)=x
theta1(x)=alpha[2]
theta2(x)=alpha[2]^2(-(27/2)a0/(-3a1+a2^2)^2+(9/2)a1 a2/(-3a1+a2^2)^2-a2^3/(-3a1+a2^2)^2+
(9/2)alpha[1]/(-3a1+a2^2)^2-27a0 z[3]/(-3a1+a2^2)^2+9a1 a2 z[3]/(-3a1+a2^2)^2-
2a2^3z[3]/(-3a1+a2^2)^2)
g2(x)=9a1^2x/(-3a1+a2^2)^2-6a1 a2^2x/(-3a1+a2^2)^2+a2^4x/(-3a1+a2^2)^2+9a1^2alpha[2]/(-3a1+a2^2)^2-
6a1 a2^2alpha[2]/(-3a1+a2^2)^2+a2^4alpha[2]/(-3a1+a2^2)^2-(27/2)a0 alpha[2]^2/(-3a1+a2^2)^2+
(9/2)a1 a2 alpha[2]^2/(-3a1+a2^2)^2-a2^3alpha[2]^2/(-3a1+a2^2)^2+(9/2)alpha[1]alpha[2]^2/(-3a1+a2^2)^2-
27a0 alpha[2]^2z[3]/(-3a1+a2^2)^2+9a1 a2 alpha[2]^2z[3]/(-3a1+a2^2)^2-2a2^3alpha[2]^2z[3]/(-3a1+a2^2)^2
List of alpha :
{alpha[1], 27a0^2+4a1^3-18a0 a1 a2-a1^2a2^2+4a0 a2^3+alpha[1]^2}
{z[3], 1+z[3]+z[3]^2}
{alpha[2], -(3/2)a0+(1/2)a1 a2-(1/9)a2^3-(1/2)alpha[1]+alpha[2]^3-3a0 z[3]+
a1 a2 z[3]-(2/9)a2^3z[3]}

```


$$\begin{aligned}
X[1] &= -3a_1^2a_2/(-3a_1+a_2^2)^2+2a_1a_2^3/(-3a_1+a_2^2)^2-(1/3)a_2^5/(-3a_1+a_2^2)^2-3a_1^2\alpha[2]/(-3a_1+a_2^2)^2+ \\
& 2a_1a_2^2\alpha[2]/(-3a_1+a_2^2)^2-(1/3)a_2^4\alpha[2]/(-3a_1+a_2^2)^2-3\alpha[1]\alpha[2]^2/(-3a_1+a_2^2)^2+ \\
& 3a_1^2\alpha[2]z[3]/(-3a_1+a_2^2)^2-2a_1a_2^2\alpha[2]z[3]/(-3a_1+a_2^2)^2+(1/3)a_2^4\alpha[2]z[3]/(-3a_1+a_2^2)^2+ \\
& (27/2)a_0\alpha[2]^2z[3]/(-3a_1+a_2^2)^2-(9/2)a_1a_2\alpha[2]^2z[3]/(-3a_1+a_2^2)^2 \\
& +a_2^3\alpha[2]^2z[3]/(-3a_1+a_2^2)^2-(3/2)\alpha[1]\alpha[2]^2z[3]/(-3a_1+a_2^2)^2 \\
X[2] &= -3a_1^2a_2/(-3a_1+a_2^2)^2+2a_1a_2^3/(-3a_1+a_2^2)^2-(1/3)a_2^5/(-3a_1+a_2^2)^2+6a_1^2\alpha[2]/(-3a_1+a_2^2)^2- \\
& 4a_1a_2^2\alpha[2]/(-3a_1+a_2^2)^2+(2/3)a_2^4\alpha[2]/(-3a_1+a_2^2)^2-(27/2)a_0\alpha[2]^2/(-3a_1+a_2^2)^2+ \\
& (9/2)a_1a_2\alpha[2]^2/(-3a_1+a_2^2)^2-a_2^3\alpha[2]^2/(-3a_1+a_2^2)^2+(3/2)\alpha[1]\alpha[2]^2/(-3a_1+a_2^2)^2+ \\
& 3a_1^2\alpha[2]z[3]/(-3a_1+a_2^2)^2-2a_1a_2^2\alpha[2]z[3]/(-3a_1+a_2^2)^2+(1/3)a_2^4\alpha[2]z[3]/(-3a_1+a_2^2)^2- \\
& (27/2)a_0\alpha[2]^2z[3]/(-3a_1+a_2^2)^2+(9/2)a_1a_2\alpha[2]^2z[3]/(-3a_1+a_2^2)^2- \\
& a_2^3\alpha[2]^2z[3]/(-3a_1+a_2^2)^2-(3/2)\alpha[1]\alpha[2]^2z[3]/(-3a_1+a_2^2)^2 \\
X[3] &= -3a_1^2a_2/(-3a_1+a_2^2)^2+2a_1a_2^3/(-3a_1+a_2^2)^2-(1/3)a_2^5/(-3a_1+a_2^2)^2-3a_1^2\alpha[2]/(-3a_1+a_2^2)^2+ \\
& 2a_1a_2^2\alpha[2]/(-3a_1+a_2^2)^2-(1/3)a_2^4\alpha[2]/(-3a_1+a_2^2)^2+(27/2)a_0\alpha[2]^2/(-3a_1+a_2^2)^2- \\
& (9/2)a_1a_2\alpha[2]^2/(-3a_1+a_2^2)^2+a_2^3\alpha[2]^2/(-3a_1+a_2^2)^2+(3/2)\alpha[1]\alpha[2]^2/(-3a_1+a_2^2)^2- \\
& 6a_1^2\alpha[2]z[3]/(-3a_1+a_2^2)^2+4a_1a_2^2\alpha[2]z[3]/(-3a_1+a_2^2)^2-(2/3)a_2^4\alpha[2]z[3]/(-3a_1+a_2^2)^2+ \\
& 3\alpha[1]\alpha[2]^2z[3]/(-3a_1+a_2^2)^2 \\
(x-X[1])(x-X[2])(x-X[3]) &= a_0+a_1x+a_2x^2+x^3
\end{aligned}$$

入力要求“Output file name : ”に対して“solution1.txt”を入力すると，ファイルsolution1.txtに以下の計算結果が書き込まれる。

$$\begin{aligned}
fx &= a_0+a_1x+a_2x^2+x^3; \\
ListOfAlpha &= \{ \alpha[1], 27a_0^2+4a_1^3-18a_0a_1a_2-a_1^2a_2^2+4a_0a_2^3+\alpha[1]^2\}, \\
& \{ z[3], 1+z[3]+z[3]^2\}, \{ \alpha[2], (-3a_0)/2+(a_1a_2)/2-a_2^3/9-\alpha[1]/2+ \\
& \alpha[2]^3-3a_0z[3]+a_1a_2z[3]-(2a_2^3z[3])/9\} \}; \\
X[1] &= (-3a_1^2a_2)/(-3a_1+a_2^2)^2+(2a_1a_2^3)/(-3a_1+a_2^2)^2-a_2^5/(3*(-3a_1+a_2^2)^2)- \\
& (3a_1^2\alpha[2])/(-3a_1+a_2^2)^2+(2a_1a_2^2\alpha[2])/(-3a_1+a_2^2)^2- \\
& (a_2^4\alpha[2])/ (3*(-3a_1+a_2^2)^2)-(3\alpha[1]\alpha[2]^2)/(-3a_1+a_2^2)^2+ \\
& (3a_1^2\alpha[2]z[3])/(-3a_1+a_2^2)^2-(2a_1a_2^2\alpha[2]z[3])/(-3a_1+a_2^2)^2+ \\
& (a_2^4\alpha[2]z[3])/ (3*(-3a_1+a_2^2)^2)+(27a_0\alpha[2]^2z[3])/(2*(-3a_1+a_2^2)^2)- \\
& (9a_1a_2\alpha[2]^2z[3])/(2*(-3a_1+a_2^2)^2)+(a_2^3\alpha[2]^2z[3])/(-3a_1+a_2^2)^2- \\
& (3\alpha[1]\alpha[2]^2z[3])/(2*(-3a_1+a_2^2)^2); \\
X[2] &= (-3a_1^2a_2)/(-3a_1+a_2^2)^2+(2a_1a_2^3)/(-3a_1+a_2^2)^2-a_2^5/(3*(-3a_1+a_2^2)^2)+ \\
& (6a_1^2\alpha[2])/(-3a_1+a_2^2)^2-(4a_1a_2^2\alpha[2])/(-3a_1+a_2^2)^2+ \\
& (2a_2^4\alpha[2])/ (3*(-3a_1+a_2^2)^2)-(27a_0\alpha[2]^2)/ (2*(-3a_1+a_2^2)^2)+ \\
& (9a_1a_2\alpha[2]^2)/ (2*(-3a_1+a_2^2)^2)-(a_2^3\alpha[2]^2)/(-3a_1+a_2^2)^2+ \\
& (3\alpha[1]\alpha[2]^2)/ (2*(-3a_1+a_2^2)^2)+(3a_1^2\alpha[2]z[3])/(-3a_1+a_2^2)^2- \\
& (2a_1a_2^2\alpha[2]z[3])/(-3a_1+a_2^2)^2+(a_2^4\alpha[2]z[3])/ (3*(-3a_1+a_2^2)^2)- \\
& (27a_0\alpha[2]^2z[3])/(2*(-3a_1+a_2^2)^2)+(9a_1a_2\alpha[2]^2z[3])/(2*(-3a_1+a_2^2)^2)- \\
& (a_2^3\alpha[2]^2z[3])/(-3a_1+a_2^2)^2-(3\alpha[1]\alpha[2]^2z[3])/(2*(-3a_1+a_2^2)^2); \\
X[3] &= (-3a_1^2a_2)/(-3a_1+a_2^2)^2+(2a_1a_2^3)/(-3a_1+a_2^2)^2-a_2^5/(3*(-3a_1+a_2^2)^2)- \\
& (3a_1^2\alpha[2])/(-3a_1+a_2^2)^2+(2a_1a_2^2\alpha[2])/(-3a_1+a_2^2)^2- \\
& (a_2^4\alpha[2])/ (3*(-3a_1+a_2^2)^2)+(27a_0\alpha[2]^2)/ (2*(-3a_1+a_2^2)^2)- \\
& (9a_1a_2\alpha[2]^2)/ (2*(-3a_1+a_2^2)^2)+(a_2^3\alpha[2]^2)/(-3a_1+a_2^2)^2+ \\
& (3\alpha[1]\alpha[2]^2)/ (2*(-3a_1+a_2^2)^2)-(6a_1^2\alpha[2]z[3])/(-3a_1+a_2^2)^2+ \\
& (4a_1a_2^2\alpha[2]z[3])/(-3a_1+a_2^2)^2-(2a_2^4\alpha[2]z[3])/ (3*(-3a_1+a_2^2)^2)+ \\
& (3\alpha[1]\alpha[2]^2z[3])/(-3a_1+a_2^2)^2;
\end{aligned}$$

上記の計算結果も含めて、以下に9つの計算例(計算不可の場合もあり)を示す。

(例1) $f(x)=x^3+a_2x^2+a_1x+a_0$ の場合

$$\alpha_1^2 - (-27a_0^2 - 4a_1^3 + 18a_0a_1a_2 + a_1^2a_2^2 - 4a_0a_2^3) = 0 \quad (14.1)$$

$$\zeta_3^2 + \zeta_3 + 1 = 0 \quad (14.2)$$

$$\alpha_2^3 - \{(3/2)a_0 - (1/2)a_1a_2 + (1/9)a_2^3 + (1/2)\alpha_1 + 3a_0\zeta_3 - a_1a_2\zeta_3 + (2/9)a_2^3\zeta_3\} = 0 \quad (14.3)$$

$$x_1 = (1/3) \{-a_2 - \alpha_2(1 - \zeta_3)\} + \alpha_2^2 \{(27a_0 - 9a_1a_2 + 2a_2^3)\zeta_3 - 3\alpha_1(2 + \zeta_3)\} / D \quad (14.4)$$

$$x_2 = (1/3) \{-a_2 + \alpha_2(2 + \zeta_3)\} + \alpha_2^2 \{-(27a_0 - 9a_1a_2 + 2a_2^3)(1 + \zeta_3) + 3\alpha_1(1 - \zeta_3)\} / D \quad (14.5)$$

$$x_3 = (1/3) \{-a_2 - \alpha_2(1 + 2\zeta_3)\} + \alpha_2^2 \{(27a_0 - 9a_1a_2 + 2a_2^3) + 3\alpha_1(1 + 2\zeta_3)\} / D \quad (14.6)$$

$$D = 2(3a_1 - a_2^2)^2 \quad (14.7)$$

(例2) $f(x)=x^4+a_2x^2+a_0$ の場合

$$\alpha_1^2 - (-36a_0 + 9a_2^2) = 0 \quad (14.8)$$

$$\alpha_2^2 - \{-2a_2 + (2/3)\alpha_1\} = 0 \quad (14.9)$$

$$\alpha_3^2 - \{-2a_2 - (2/3)\alpha_1\} = 0 \quad (14.10)$$

$$x_1 = (1/2)\alpha_2 \quad (14.11)$$

$$x_2 = -(1/2)\alpha_2 \quad (14.12)$$

$$x_3 = (1/2)\alpha_3 \quad (14.13)$$

$$x_4 = -(1/2)\alpha_3 \quad (14.14)$$

(例3) $f(x)=x^4+a_2x^2+a_1x+a_0$ の場合

$f(x)$ の係数が数値でなく文字のため、計算途中の結果が非常に長い式となり、計算できなかった。

(例4) $f(x)=x^4+2x^3+3x^2+4x+5$ の場合

既に $\alpha_1, \zeta_3, \alpha_2, \alpha_3, \alpha_4$ の条件式は(12.13), (12.23), (12.27), (12.39), (12.49)で示した。 x_1, x_2, x_3, x_4 は(13.1)-(13.4)で示した。

(例5) $f(x)=x^5+2x^3+4x^2-x+4$ の場合

$$\alpha_1^2 - 8712 = 0 \quad (14.15)$$

$$\alpha_2^2 - \{-440 - (2/3)\alpha_1\} = 0 \quad (14.16)$$

$$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0 \quad (14.17)$$

$$\begin{aligned} \alpha_3^5 - \{ & -3029/5 - (1042/165)\alpha_1 + (35067/1750)\alpha_2 + (1231/5775)\alpha_1\alpha_2 - (6058/5)\zeta_5 \\ & - (2084/165)\alpha_1\zeta_5 - (4901/5)\zeta_5^2 - (562/55)\alpha_1\zeta_5^2 - (56741/1750)\alpha_2\zeta_5^2 - (7967/23100)\alpha_1\alpha_2\zeta_5^2 \\ & - (1157/5)\zeta_5^3 - (398/165)\alpha_1\zeta_5^3 - (56741/1750)\alpha_2\zeta_5^3 - (7967/23100)\alpha_1\alpha_2\zeta_5^3 \} = 0 \end{aligned} \quad (14.18)$$

$$\begin{aligned} x_1 = & (7/5)\alpha_3 - (605/169)\alpha_3^2 - (175/11154)\alpha_1\alpha_3^2 + (659/2366)\alpha_2\alpha_3^2 + (158/39039)\alpha_1\alpha_2\alpha_3^2 + (255/169)\alpha_3^3 \\ & + (2987/48334)\alpha_1\alpha_3^3 + (3215/2197)\alpha_2\alpha_3^3 + (2325/96668)\alpha_1\alpha_2\alpha_3^3 - (638370/199927)\alpha_2\alpha_3^4 \\ & + (825115/13195182)\alpha_1\alpha_2\alpha_3^4 - (1/5)\alpha_3\zeta_5 + (385/169)\alpha_3^2\zeta_5 + (35/3718)\alpha_1\alpha_3^2\zeta_5 + (31/182)\alpha_2\alpha_3^2\zeta_5 \\ & + (131/52052)\alpha_1\alpha_2\alpha_3^2\zeta_5 - (5355/2197)\alpha_3^3\zeta_5 - (4841/48334)\alpha_1\alpha_3^3\zeta_5 + (8620/15379)\alpha_2\alpha_3^3\zeta_5 \\ & + (18625/2030028)\alpha_1\alpha_2\alpha_3^3\zeta_5 + (3554375/28561)\alpha_3^4\zeta_5 + (82000/314171)\alpha_1\alpha_3^4\zeta_5 - (243935/399854)\alpha_2\alpha_3^4\zeta_5 \\ & + (105045/8796788)\alpha_1\alpha_2\alpha_3^4\zeta_5 + (6/5)\alpha_3\zeta_5^2 - (605/169)\alpha_3^2\zeta_5^2 - (175/11154)\alpha_1\alpha_3^2\zeta_5^2 + (21/338)\alpha_2\alpha_3^2\zeta_5^2 \\ & + (1/1014)\alpha_1\alpha_2\alpha_3^2\zeta_5^2 + (5355/2197)\alpha_3^3\zeta_5^2 + (4841/48334)\alpha_1\alpha_3^3\zeta_5^2 + (8620/15379)\alpha_2\alpha_3^3\zeta_5^2 \\ & + (18625/2030028)\alpha_1\alpha_2\alpha_3^3\zeta_5^2 - (2197250/28561)\alpha_3^4\zeta_5^2 - (152000/942513)\alpha_1\alpha_3^4\zeta_5^2 - (319185/199927)\alpha_2\alpha_3^4\zeta_5^2 \\ & + (825115/26390364)\alpha_1\alpha_2\alpha_3^4\zeta_5^2 + (3/5)\alpha_3\zeta_5^3 + (31/91)\alpha_2\alpha_3^2\zeta_5^3 + (131/26026)\alpha_1\alpha_2\alpha_3^2\zeta_5^3 - (255/169)\alpha_3^3\zeta_5^3 \\ & - (2987/48334)\alpha_1\alpha_3^3\zeta_5^3 + (3215/2197)\alpha_2\alpha_3^3\zeta_5^3 + (2325/96668)\alpha_1\alpha_2\alpha_3^3\zeta_5^3 + (3554375/28561)\alpha_3^4\zeta_5^3 \\ & + (82000/314171)\alpha_1\alpha_3^4\zeta_5^3 - (1032805/399854)\alpha_2\alpha_3^4\zeta_5^3 + (1335095/26390364)\alpha_1\alpha_2\alpha_3^4\zeta_5^3 \end{aligned} \quad (14.19)$$

$$\begin{aligned}
x_2 = & (8/5)\alpha_3 - (990/169)\alpha_3^2 - (140/5577)\alpha_1\alpha_3^2 - (128/1183)\alpha_2\alpha_3^2 - (239/156156)\alpha_1\alpha_2\alpha_3^2 - (8670/2197)\alpha_3^3 \\
& - (3914/24167)\alpha_1\alpha_3^3 + (13885/15379)\alpha_2\alpha_3^3 + (7550/507507)\alpha_1\alpha_2\alpha_3^3 - (3554375/28561)\alpha_3^4 \\
& - (82000/314171)\alpha_1\alpha_3^4 + (1032805/399854)\alpha_2\alpha_3^4 - (1335095/26390364)\alpha_1\alpha_2\alpha_3^4 - (1/5)\alpha_3\zeta_5 - (385/169)\alpha_3^2\zeta_5 \\
& - (35/3718)\alpha_1\alpha_3^2\zeta_5 + (31/182)\alpha_2\alpha_3^2\zeta_5 + (131/52052)\alpha_1\alpha_2\alpha_3^2\zeta_5 - (5355/2197)\alpha_3^3\zeta_5 - (4841/48334)\alpha_1\alpha_3^3\zeta_5 \\
& - (8620/15379)\alpha_2\alpha_3^3\zeta_5 - (18625/2030028)\alpha_1\alpha_2\alpha_3^3\zeta_5 - (3554375/28561)\alpha_3^4\zeta_5 - (82000/314171)\alpha_1\alpha_3^4\zeta_5 \\
& - (243935/399854)\alpha_2\alpha_3^4\zeta_5 + (105045/8796788)\alpha_1\alpha_2\alpha_3^4\zeta_5 - (4/5)\alpha_3\zeta_5^2 - (385/169)\alpha_3^2\zeta_5^2 - (35/3718)\alpha_1\alpha_3^2\zeta_5^2 \\
& - (31/182)\alpha_2\alpha_3^2\zeta_5^2 - (131/52052)\alpha_1\alpha_2\alpha_3^2\zeta_5^2 - (2040/2197)\alpha_3^3\zeta_5^2 - (927/24167)\alpha_1\alpha_3^3\zeta_5^2 \\
& + (13885/15379)\alpha_2\alpha_3^3\zeta_5^2 + (7550/507507)\alpha_1\alpha_2\alpha_3^3\zeta_5^2 + (394435/199927)\alpha_2\alpha_3^4\zeta_5^2 \\
& - (254990/6597591)\alpha_1\alpha_2\alpha_3^4\zeta_5^2 - (7/5)\alpha_3\zeta_5^3 - (990/169)\alpha_3^2\zeta_5^3 - (140/5577)\alpha_1\alpha_3^2\zeta_5^3 + (128/1183)\alpha_2\alpha_3^2\zeta_5^3 \\
& + (239/156156)\alpha_1\alpha_2\alpha_3^2\zeta_5^3 - (10710/2197)\alpha_3^3\zeta_5^3 - (4841/24167)\alpha_1\alpha_3^3\zeta_5^3 - (5751625/28561)\alpha_3^4\zeta_5^3 \\
& - (398000/942513)\alpha_1\alpha_3^4\zeta_5^3 + (394435/399854)\alpha_2\alpha_3^4\zeta_5^3 - (127495/6597591)\alpha_1\alpha_2\alpha_3^4\zeta_5^3 \quad (14.20)
\end{aligned}$$

$$\begin{aligned}
x_3 = & (3/5)\alpha_3 + (605/169)\alpha_3^2 + (175/11154)\alpha_1\alpha_3^2 + (659/2366)\alpha_2\alpha_3^2 + (158/39039)\alpha_1\alpha_2\alpha_3^2 + (10710/2197)\alpha_3^3 \\
& + (4841/24167)\alpha_1\alpha_3^3 + (3554375/28561)\alpha_3^4 + (82000/314171)\alpha_1\alpha_3^4 + (1032805/399854)\alpha_2\alpha_3^4 \\
& - (1335095/26390364)\alpha_1\alpha_2\alpha_3^4 + (4/5)\alpha_3\zeta_5 + (605/169)\alpha_3^2\zeta_5 + (175/11154)\alpha_1\alpha_3^2\zeta_5 - (21/338)\alpha_2\alpha_3^2\zeta_5 \\
& - (1/1014)\alpha_1\alpha_2\alpha_3^2\zeta_5 + (2040/2197)\alpha_3^3\zeta_5 + (927/24167)\alpha_1\alpha_3^3\zeta_5 + (13885/15379)\alpha_2\alpha_3^3\zeta_5 \\
& + (7550/507507)\alpha_1\alpha_2\alpha_3^3\zeta_5 - (2197250/28561)\alpha_3^4\zeta_5 - (152000/942513)\alpha_1\alpha_3^4\zeta_5 + (319185/199927)\alpha_2\alpha_3^4\zeta_5 \\
& - (825115/26390364)\alpha_1\alpha_2\alpha_3^4\zeta_5 - (4/5)\alpha_3\zeta_5^2 + (256/1183)\alpha_2\alpha_3^2\zeta_5^2 + (239/78078)\alpha_1\alpha_2\alpha_3^2\zeta_5^2 + (5355/2197)\alpha_3^3\zeta_5^2 \\
& + (4841/48334)\alpha_1\alpha_3^3\zeta_5^2 - (8620/15379)\alpha_2\alpha_3^3\zeta_5^2 - (18625/2030028)\alpha_1\alpha_2\alpha_3^3\zeta_5^2 + (3554375/28561)\alpha_3^4\zeta_5^2 \\
& + (82000/314171)\alpha_1\alpha_3^4\zeta_5^2 + (243935/399854)\alpha_2\alpha_3^4\zeta_5^2 - (105045/8796788)\alpha_1\alpha_2\alpha_3^4\zeta_5^2 + (3/5)\alpha_3\zeta_5^3 \\
& + (990/169)\alpha_3^2\zeta_5^3 + (140/5577)\alpha_1\alpha_3^2\zeta_5^3 + (128/1183)\alpha_2\alpha_3^2\zeta_5^3 + (239/156156)\alpha_1\alpha_2\alpha_3^2\zeta_5^3 + (8670/2197)\alpha_3^3\zeta_5^3 \\
& + (3914/24167)\alpha_1\alpha_3^3\zeta_5^3 + (13885/15379)\alpha_2\alpha_3^3\zeta_5^3 + (7550/507507)\alpha_1\alpha_2\alpha_3^3\zeta_5^3 + (638370/199927)\alpha_2\alpha_3^4\zeta_5^3 \\
& - (825115/13195182)\alpha_1\alpha_2\alpha_3^4\zeta_5^3 \quad (14.21)
\end{aligned}$$

$$\begin{aligned}
x_4 = & (7/5)\alpha_3 - (31/91)\alpha_2\alpha_3^2 - (131/26026)\alpha_1\alpha_2\alpha_3^2 - (8670/2197)\alpha_3^3 - (3914/24167)\alpha_1\alpha_3^3 - (13885/15379)\alpha_2\alpha_3^3 \\
& - (7550/507507)\alpha_1\alpha_2\alpha_3^3 + (5751625/28561)\alpha_3^4 + (398000/942513)\alpha_1\alpha_3^4 - (394435/399854)\alpha_2\alpha_3^4 \\
& + (127495/6597591)\alpha_1\alpha_2\alpha_3^4 + (4/5)\alpha_3\zeta_5 - (605/169)\alpha_3^2\zeta_5 - (175/11154)\alpha_1\alpha_3^2\zeta_5 - (21/338)\alpha_2\alpha_3^2\zeta_5 \\
& - (1/1014)\alpha_1\alpha_2\alpha_3^2\zeta_5 + (2040/2197)\alpha_3^3\zeta_5 + (927/24167)\alpha_1\alpha_3^3\zeta_5 - (13885/15379)\alpha_2\alpha_3^3\zeta_5 \\
& - (7550/507507)\alpha_1\alpha_2\alpha_3^3\zeta_5 + (2197250/28561)\alpha_3^4\zeta_5 + (152000/942513)\alpha_1\alpha_3^4\zeta_5 + (319185/199927)\alpha_2\alpha_3^4\zeta_5 \\
& - (825115/26390364)\alpha_1\alpha_2\alpha_3^4\zeta_5 + (1/5)\alpha_3\zeta_5^2 + (385/169)\alpha_3^2\zeta_5^2 + (35/3718)\alpha_1\alpha_3^2\zeta_5^2 - (31/182)\alpha_2\alpha_3^2\zeta_5^2 \\
& - (131/52052)\alpha_1\alpha_2\alpha_3^2\zeta_5^2 - (510/169)\alpha_3^3\zeta_5^2 - (2987/24167)\alpha_1\alpha_3^3\zeta_5^2 + (2197250/28561)\alpha_3^4\zeta_5^2 \\
& + (152000/942513)\alpha_1\alpha_3^4\zeta_5^2 - (319185/199927)\alpha_2\alpha_3^4\zeta_5^2 + (825115/26390364)\alpha_1\alpha_2\alpha_3^4\zeta_5^2 + (8/5)\alpha_3\zeta_5^3 \\
& - (605/169)\alpha_3^2\zeta_5^3 - (175/11154)\alpha_1\alpha_3^2\zeta_5^3 - (659/2366)\alpha_2\alpha_3^2\zeta_5^3 - (158/39039)\alpha_1\alpha_2\alpha_3^2\zeta_5^3 - (255/169)\alpha_3^3\zeta_5^3 \\
& - (2987/48334)\alpha_1\alpha_3^3\zeta_5^3 - (3215/2197)\alpha_2\alpha_3^3\zeta_5^3 - (2325/96668)\alpha_1\alpha_2\alpha_3^3\zeta_5^3 + (5751625/28561)\alpha_3^4\zeta_5^3 \\
& + (398000/942513)\alpha_1\alpha_3^4\zeta_5^3 + (394435/399854)\alpha_2\alpha_3^4\zeta_5^3 - (127495/6597591)\alpha_1\alpha_2\alpha_3^4\zeta_5^3 \quad (14.22)
\end{aligned}$$

$$\begin{aligned}
x_5 = & (3/5)\alpha_3 + (990/169)\alpha_3^2 + (140/5577)\alpha_1\alpha_3^2 - (128/1183)\alpha_2\alpha_3^2 - (239/156156)\alpha_1\alpha_2\alpha_3^2 + (255/169)\alpha_3^3 \\
& + (2987/48334)\alpha_1\alpha_3^3 - (3215/2197)\alpha_2\alpha_3^3 - (2325/96668)\alpha_1\alpha_2\alpha_3^3 - (5751625/28561)\alpha_3^4 \\
& - (398000/942513)\alpha_1\alpha_3^4 - (394435/399854)\alpha_2\alpha_3^4 + (127495/6597591)\alpha_1\alpha_2\alpha_3^4 - (6/5)\alpha_3\zeta_5 - (256/1183)\alpha_2\alpha_3^2\zeta_5 \\
& - (239/78078)\alpha_1\alpha_2\alpha_3^2\zeta_5 + (510/169)\alpha_3^3\zeta_5 + (2987/24167)\alpha_1\alpha_3^3\zeta_5 - (394435/199927)\alpha_2\alpha_3^3\zeta_5 \\
& + (254990/6597591)\alpha_1\alpha_2\alpha_3^3\zeta_5 + (1/5)\alpha_3\zeta_5^2 + (605/169)\alpha_3^2\zeta_5^2 + (175/11154)\alpha_1\alpha_3^2\zeta_5^2 + (21/338)\alpha_2\alpha_3^2\zeta_5^2 \\
& + (1/1014)\alpha_1\alpha_2\alpha_3^2\zeta_5^2 - (2040/2197)\alpha_3^3\zeta_5^2 - (927/24167)\alpha_1\alpha_3^3\zeta_5^2 - (13885/15379)\alpha_2\alpha_3^3\zeta_5^2 \\
& - (7550/507507)\alpha_1\alpha_2\alpha_3^3\zeta_5^2 - (3554375/28561)\alpha_3^4\zeta_5^2 - (82000/314171)\alpha_1\alpha_3^4\zeta_5^2 + (243935/399854)\alpha_2\alpha_3^4\zeta_5^2 \\
& - (105045/8796788)\alpha_1\alpha_2\alpha_3^4\zeta_5^2 - (7/5)\alpha_3\zeta_5^3 + (605/169)\alpha_3^2\zeta_5^3 + (175/11154)\alpha_1\alpha_3^2\zeta_5^3 - (659/2366)\alpha_2\alpha_3^2\zeta_5^3 \\
& - (158/39039)\alpha_1\alpha_2\alpha_3^2\zeta_5^3 + (8670/2197)\alpha_3^3\zeta_5^3 + (3914/24167)\alpha_1\alpha_3^3\zeta_5^3 - (13885/15379)\alpha_2\alpha_3^3\zeta_5^3 \\
& - (7550/507507)\alpha_1\alpha_2\alpha_3^3\zeta_5^3 - (3554375/28561)\alpha_3^4\zeta_5^3 - (82000/314171)\alpha_1\alpha_3^4\zeta_5^3 - (1032805/399854)\alpha_2\alpha_3^4\zeta_5^3 \\
& + (1335095/26390364)\alpha_1\alpha_2\alpha_3^4\zeta_5^3 \quad (14.23)
\end{aligned}$$

(追記) 第15節の(例1)によると, 根 x_1, x_2, x_3, x_4, x_5 は次式で与えられる。

$$\begin{aligned} x_1 &= A+B+C+D, \quad x_2 = \zeta_5 A + \zeta_5^2 B + \zeta_5^3 C + \zeta_5^4 D, \quad x_3 = \zeta_5^2 A + \zeta_5^4 B + \zeta_5 C + \zeta_5^3 D \\ x_4 &= \zeta_5^3 A + \zeta_5 B + \zeta_5^4 C + \zeta_5^2 D, \quad x_5 = \zeta_5^4 A + \zeta_5^3 B + \zeta_5^2 C + \zeta_5 D \end{aligned} \quad (14.24)$$

ここで

$$A^5 = -(13+4\sqrt{10})/25 - \sqrt{11(19850+6277\sqrt{10})}/625 \quad (14.25)$$

$$B^5 = -(13-4\sqrt{10})/25 - \sqrt{11(19850-6277\sqrt{10})}/625 \quad (14.26)$$

$$C^5 = -(13-4\sqrt{10})/25 + \sqrt{11(19850-6277\sqrt{10})}/625 \quad (14.27)$$

$$D^5 = -(13+4\sqrt{10})/25 + \sqrt{11(19850+6277\sqrt{10})}/625 \quad (14.28)$$

A, B, C, D は各々 A^5, B^5, C^5, D^5 の実数の5乗根を選ぶ。

(例6) $f(x) = x^5 + a_3 x^3 + (a_3^2/5)x + a_0$ の場合

第10節の(例6)の計算が未了のため, 可解であるかどうかは不明で, 根の計算はできない。

(追記) 第15節の(3)の場合によると, 根 x_1, x_2, x_3, x_4, x_5 は次式で与えられる。

$$x_1 = A+D, \quad x_2 = \zeta_5 A + \zeta_5^4 D, \quad x_3 = \zeta_5^2 A + \zeta_5^3 D, \quad x_4 = \zeta_5^3 A + \zeta_5^2 D, \quad x_5 = \zeta_5^4 A + \zeta_5 D \quad (14.29)$$

ここで

$$A^5 = -a_0/2 + \sqrt{(a_0/2)^2 + (a_3/5)^5}, \quad D^5 = -a_0/2 - \sqrt{(a_0/2)^2 + (a_3/5)^5} \quad (14.30)$$

A は A^5 の5乗根のうち, 任意の1つを選ぶ。 D は D^5 の5乗根のうち, $AD = -a_3/5$ を満たすものを選ぶ。

(例7) $f(x) = x^5 + 2x^4 + 3x^3 + 4x^2 + 5x + 6$ の場合

第10節の(例7)でガロア群が可解でなかったため, べき根で表される根は存在しない。

(例8) $f(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7$ の場合

第10節の(例8)の計算が未了のため, 可解であるかどうかは不明で, 根の計算はできない。

(例9) $f(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ の場合

本節のプログラムで計算するには, 第10節のプログラムの計算結果が必要であるが, 本例にはそれがないので, (10.38)-(10.43)をもとにして, 以下の入力ファイルを作る。

```
fx=x^16+x^15+x^14+x^13+x^12+x^11+x^10+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1;
For[i=1,i<=16,i++,m[i]=If[i==1,1,0]];
gx=fx;
For[i=1,i<=16,i++,X[i]=If[i<16,v^i,-Sum[v^j,{j,0,15}]]];
G={};
Gi=Table[i,{i,1,16}];
For[i=1,i<=16,i++,
  AppendTo[G,Gi];
  Gi=Table[Mod[3*Part[Gi,j],17],{j,1,16}]]];
Gs={{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16},
  {1,3,5,7,9,11,13,15},{1,5,9,13},{1,9},{1}};
```

これを本節のプログラムで読み込むようにすると、以下の計算結果が得られる。

$$\alpha_1^2 - 17/4 = 0 \quad (14.31)$$

$$\alpha_2^2 - \{17/8 + (1/4)\alpha_1\} = 0 \quad (14.32)$$

$$\alpha_3^2 - \{17/16 - (3/8)\alpha_1 + (3/8)\alpha_2 - (1/4)\alpha_1\alpha_2\} = 0 \quad (14.33)$$

$$\alpha_4^2 - \{-17/32 - (1/16)\alpha_1 + (1/8)\alpha_2 + (1/16)\alpha_3 + (1/8)\alpha_1\alpha_3 + (1/4)\alpha_2\alpha_3\} = 0 \quad (14.34)$$

$$x_1 = -1/16 - (1/8)\alpha_1 - (1/4)\alpha_2 - (1/2)\alpha_3 - \alpha_4 \quad (14.35)$$

$x_2, x_3, \dots, x_{16}$ は省略するが、(14.31)–(14.34)より $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ は $2 \times 2 \times 2 \times 2 = 16$ 通りの値を取るの、これらを(14.35)に代入すれば、すべての根が求められる。

《計算時間》

プログラムの各所にPrint[Date[]]を挿入し、その時点での日付と時刻を印字することにより、各段階の所要時間を調べた。下表において、プログラム(1)は第1部で示したもの(ガロア群を計算する)、プログラム(2)は第2部で示したもの(可解な方程式を解く)である。使用したパソコンの仕様はCPU 2.40GHz, RAM 3.86GBである。

	プログラム(1)			プログラム(2)
	最小多項式 $g(x)$	根 x_i の多項式表現	ガロア群と組成列	根 x_i のべき根表現
(例1)	0秒	0秒	0秒	0秒
(例2)	0秒	9秒	0秒	1秒
(例3)	2秒	12分55秒	0秒	—
(例4)	0秒	1秒	0秒	1分30秒
(例5)	13秒	24分35秒	1分57秒	4分50秒
(例6)	3分19秒	計算不可	計算不可	—
(例7)	15秒	26分09秒	12秒	—
(例8)	計算不可	計算不可	計算不可	—
(例9)	計算不可	計算不可	計算不可	6秒

$$(例1) f(x) = x^3 + a_2x^2 + a_1x + a_0$$

$$(例2) f(x) = x^4 + a_2x^2 + a_0$$

$$(例3) f(x) = x^4 + a_2x^2 + a_1x + a_0$$

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

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

$$(例6) f(x) = x^5 + a_3x^3 + (a_3^2/5)x + a_0$$

$$(例7) f(x) = x^5 + 2x^4 + 3x^3 + 4x^2 + 5x + 6$$

$$(例8) f(x) = x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7$$

$$(例9) f(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

《べき根の選び方に制約のある計算例》

前節の(例4)では $f(x) = x^4 + 2x^3 + 3x^2 + 4x + 5$ の根 x_1, x_2, x_3, x_4 について、 $(x-x_1)(x-x_2)(x-x_3)(x-x_4)$ を展開して、これが $f(x)$ と一致することを確認した。つぎに、べき根 $\alpha_1, \zeta_3, \alpha_2, \alpha_3, \alpha_4$ には各々2, 2, 3, 2, 2通りの選び方があり、これに対応する $2 \times 2 \times 3 \times 2 \times 2 = 48$ 通りの x_1, x_2, x_3, x_4 について、これらがすべて $f(x)$ の根になっていることも確認した。つまり、この場合はべき根の選び方に制約はない。ところが、以下に示す計算例では、べき根の選び方によっては $(x-x_1)(x-x_2)\cdots(x-x_n)$ が $f(x)$ と一致せず、これに対応する $x_1, x_2, \dots, x_n$ は $f(x)$ の根とはならない。

(例10) $f(x)=x^3-2$ の場合

計算結果は以下となる。

$$v=x_1-x_2 \quad (14.36)$$

$$g(x)=x^6+108 \quad (14.37)$$

$$G=\{\{1, 2, 3\}, \{1, 3, 2\}, \{2, 1, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{3, 2, 1\}\} \quad (14.38)$$

$$G_0=\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}, \quad G_1=\{\sigma_1, \sigma_4, \sigma_5\}, \quad G_2=\{\sigma_1\} \quad (14.39)$$

$$\alpha_1^2+108=0, \quad \zeta_3^2+\zeta_3+1=0, \quad \alpha_2^3+3-\alpha_1/2+6\zeta_3=0 \quad (14.40)$$

$$x_1=-\alpha_2/2-\alpha_1\alpha_2/36, \quad x_2=\alpha_2/2-\alpha_1\alpha_2/36, \quad x_3=\alpha_1\alpha_2/18 \quad (14.41)$$

$$(x-x_1)(x-x_2)(x-x_3)=x^3-1-(1/18)\alpha_1(1+2\zeta_3) \quad (14.42)$$

(14.42)はべき根の選び方によっては、必ずしも $(x-x_1)(x-x_2)(x-x_3)=x^3-2$ とはならない。(14.40)より α_1, α_2 には $2 \times 3 = 6$ 通りの選び方があり、各場合について x_1, x_2, x_3 を調べる。ただし、調べる場合数が多くならないように、 ζ_3 は次式に固定した。

$$\zeta_3=(-1+\sqrt{3}i)/2 \quad (14.43)$$

ここで、根の真値 X_1, X_2, X_3 は次式である。

$$X_1=\sqrt[3]{2}, \quad X_2=\sqrt[3]{2}\zeta_3, \quad X_3=\sqrt[3]{2}\zeta_3^2 \quad (14.44)$$

(1) $\alpha_1=6\sqrt{3}i$ の場合

(14.42)は $(x-x_1)(x-x_2)(x-x_3)=x^3$ となる。

(14.40)は $\alpha_2^3=0$ となる。これより、 $(x_1, x_2, x_3)=(0, 0, 0)$ となる。

(2) $\alpha_1=-6\sqrt{3}i$ の場合

(14.42)は $(x-x_1)(x-x_2)(x-x_3)=x^3-2$ となる。(14.40)は $\alpha_2^3+6\sqrt{3}i=\alpha_2^3-2(\sqrt{3}i)^3=0$ となる。

$\alpha_2=\sqrt[3]{2}\sqrt{3}i$ ならば、 $(x_1, x_2, x_3)=(X_3, X_2, X_1)$ となる。

$\alpha_2=\sqrt[3]{2}\sqrt{3}i\zeta_3$ ならば、 $(x_1, x_2, x_3)=(X_1, X_3, X_2)$ となる。

$\alpha_2=\sqrt[3]{2}\sqrt{3}i\zeta_3^2$ ならば、 $(x_1, x_2, x_3)=(X_2, X_1, X_3)$ となる。

これより、本例ではべき根の選び方に制約があり、正しい根が得られるのは(2)の場合だけである。この制約を回避する1つの方法として、 ζ_3 を付加した体上で予め $g(x)$ を因数分解しておき、ここから根の計算を始める方法がある。この方法によると、計算結果は以下となる。

$$g(x)=x^3+6(1+2\zeta_3) \quad (14.45)$$

$$G_0=\{\sigma_1, \sigma_4, \sigma_5\}, \quad G_1=\{\sigma_1\} \quad (14.46)$$

$$\zeta_3^2+\zeta_3+1=0, \quad \beta_1^3-6(1+2\zeta_3)=0 \quad (14.47)$$

$$x_1=\beta_1(-2-\zeta_3)/3, \quad x_2=\beta_1(1-\zeta_3)/3, \quad x_3=\beta_1(1+2\zeta_3)/3 \quad (14.48)$$

$$(x-x_1)(x-x_2)(x-x_3)=x^3-2 \quad (14.49)$$

(14.49)はべき根の選び方に関係なく、常に $(x-x_1)(x-x_2)(x-x_3)=x^3-2$ となる。

(14.47)は $\beta_1^3-6\sqrt{3}i=\beta_1^3+2(\sqrt{3}i)^3=0$ となる。

$\beta_1=-\sqrt[3]{2}\sqrt{3}i$ ならば、 $(x_1, x_2, x_3)=(X_2, X_3, X_1)$ となる。

$\beta_1=-\sqrt[3]{2}\sqrt{3}i\zeta_3$ ならば、 $(x_1, x_2, x_3)=(X_3, X_1, X_2)$ となる。

$\beta_1=-\sqrt[3]{2}\sqrt{3}i\zeta_3^2$ ならば、 $(x_1, x_2, x_3)=(X_1, X_2, X_3)$ となる。

この方法によれば、べき根の選び方の制約を回避することができる。

(例11) $f(x)=x^5-3$ の場合
計算結果は以下となる。

$$v=x_1-x_2+2x_3-2x_4 \quad (14.50)$$

$$g(x)=x^{20}+84403125x^{10}+253125 \quad (14.51)$$

$$G=\{\{1, 2, 3, 4, 5\}, \{1, 3, 2, 5, 4\}, \{1, 4, 5, 3, 2\}, \{1, 5, 4, 2, 3\}, \{2, 1, 4, 3, 5\}, \\ \{2, 3, 5, 4, 1\}, \{2, 4, 1, 5, 3\}, \{2, 5, 3, 1, 4\}, \{3, 1, 5, 2, 4\}, \{3, 2, 4, 5, 1\}, \\ \{3, 4, 2, 1, 5\}, \{3, 5, 1, 4, 2\}, \{4, 1, 3, 5, 2\}, \{4, 2, 5, 1, 3\}, \{4, 3, 1, 2, 5\}, \\ \{4, 5, 2, 3, 1\}, \{5, 1, 2, 4, 3\}, \{5, 2, 1, 3, 4\}, \{5, 3, 4, 1, 2\}, \{5, 4, 3, 2, 1\}\} \quad (14.52)$$

$$G_0=\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}, \sigma_{17}, \sigma_{18}, \sigma_{19}, \sigma_{20}\} \quad (14.53)$$

$$G_1=\{\sigma_1, \sigma_2, \sigma_5, \sigma_7, \sigma_9, \sigma_{12}, \sigma_{14}, \sigma_{16}, \sigma_{19}, \sigma_{20}\}, \quad G_2=\{\sigma_1, \sigma_7, \sigma_9, \sigma_{16}, \sigma_{19}\}, \quad G_3=\{\sigma_1\} \quad (14.54)$$

$$\alpha_1^2-7123887508753125/4=0, \quad \alpha_2^2+\alpha_1+84403125/2=0, \quad \zeta_5^4+\zeta_5^3+\zeta_5^2+\zeta_5+1=0 \quad (14.55)$$

$$\alpha_3^5-(15/4)(233+466\zeta_5+377\zeta_5^2+89\zeta_5^3)-(1/25164150)\alpha_1(521+1042\zeta_5+843\zeta_5^2+199\zeta_5^3) \\ -(1/4)\alpha_2+(1/377462250)\alpha_1\alpha_2(1+2\zeta_5^2+2\zeta_5^3)=0 \quad (14.56)$$

$$x_1=\alpha_3-(1/37746225)\alpha_1\alpha_3-(377/60)\alpha_2\alpha_3+(281/1887311250)\alpha_1\alpha_2\alpha_3 \quad (14.57)$$

$$x_2=-\alpha_3+(1/37746225)\alpha_1\alpha_3-(377/60)\alpha_2\alpha_3+(281/1887311250)\alpha_1\alpha_2\alpha_3 \quad (14.58)$$

$$x_3=-(3/4)\alpha_3+(1/75492450)\alpha_1\alpha_3+(329/20)\alpha_2\alpha_3-(2207/5661933750)\alpha_1\alpha_2\alpha_3 \quad (14.59)$$

$$x_4=(3/4)\alpha_3-(1/75492450)\alpha_1\alpha_3+(329/20)\alpha_2\alpha_3-(2207/5661933750)\alpha_1\alpha_2\alpha_3 \quad (14.60)$$

$$x_5=-(61/3)\alpha_1\alpha_3+(124/257360625)\alpha_1\alpha_2\alpha_3 \quad (14.61)$$

$$(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)=x^5-3/4+(1/125820750)\alpha_1(1+2\zeta_5^2+2\zeta_5^3) \\ +(1/100)\alpha_2(322+644\zeta_5-199\zeta_5^2+843\zeta_5^3) \\ +(1/1887311250)\alpha_1\alpha_2(-144-288\zeta_5+89\zeta_5^2-377\zeta_5^3) \quad (14.62)$$

(14.62)はべき根の選び方によっては、必ずしも $(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)=x^5-3$ とはならない。
(14.55), (14.56)より $\alpha_1, \alpha_2, \alpha_3$ には $2 \times 2 \times 5 = 20$ 通りの選び方があり、各場合について x_1, x_2, x_3, x_4, x_5 を調べる。ただし、調べる場合数が多くならないように、 ζ_5 は次式に固定した。

$$\zeta_5=(-1+\sqrt{5}+\sqrt{10+2\sqrt{5}i})/4 \quad (14.63)$$

ここで、根の真値 X_1, X_2, X_3, X_4, X_5 は次式である。

$$X_1=\sqrt[5]{3}, \quad X_2=\sqrt[5]{3}\zeta_5, \quad X_3=\sqrt[5]{3}\zeta_5^2, \quad X_4=\sqrt[5]{3}\zeta_5^3, \quad X_5=\sqrt[5]{3}\zeta_5^4 \quad (14.64)$$

(1) $\alpha_1=(37746225/2)\sqrt{5}$, $\alpha_2=15\sqrt{(375125+167761\sqrt{5})/2i}$ の場合

(14.62)は $(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)=x^5-3$ となる。

(14.56)は $\alpha_3^5-15\sqrt{(375125+167761\sqrt{5})/2i}=\alpha_3^5-3\{\sqrt{(25+11\sqrt{5})/2i}\}^5=0$ となる。

$\alpha_3=\sqrt[5]{3}\sqrt{(25+11\sqrt{5})/2i}$ ならば、 $(x_1, x_2, x_3, x_4, x_5)=(X_4, X_3, X_5, X_2, X_1)$ となる。

$\alpha_3=\sqrt[5]{3}\zeta_5\sqrt{(25+11\sqrt{5})/2i}$ ならば、 $(x_1, x_2, x_3, x_4, x_5)=(X_5, X_4, X_1, X_3, X_2)$ となる。

$\alpha_3=\sqrt[5]{3}\zeta_5^2\sqrt{(25+11\sqrt{5})/2i}$ ならば、 $(x_1, x_2, x_3, x_4, x_5)=(X_1, X_5, X_2, X_4, X_3)$ となる。

$\alpha_3=\sqrt[5]{3}\zeta_5^3\sqrt{(25+11\sqrt{5})/2i}$ ならば、 $(x_1, x_2, x_3, x_4, x_5)=(X_2, X_1, X_3, X_5, X_4)$ となる。

$\alpha_3=\sqrt[5]{3}\zeta_5^4\sqrt{(25+11\sqrt{5})/2i}$ ならば、 $(x_1, x_2, x_3, x_4, x_5)=(X_3, X_2, X_4, X_1, X_5)$ となる。

(2) $\alpha_1=(37746225/2)\sqrt{5}$, $\alpha_2=-15\sqrt{(375125+167761\sqrt{5})/2i}$ の場合

(14.62)は $(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)=x^5$ となる。

(14.56)は $\alpha_3^5=0$ となる。これより、 $(x_1, x_2, x_3, x_4, x_5)=(0, 0, 0, 0, 0)$ となる。

(3) $\alpha_1 = -(37746225/2)\sqrt{5}$, $\alpha_2 = 15\sqrt{(375125 - 167761\sqrt{5})/2i}$ の場合

(14. 62) は $(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5) = x^5$ となる。

(14. 56) は $\alpha_3^5 = 0$ となる。これより, $(x_1, x_2, x_3, x_4, x_5) = (0, 0, 0, 0, 0)$ となる。

(4) $\alpha_1 = -(37746225/2)\sqrt{5}$, $\alpha_2 = -15\sqrt{(375125 - 167761\sqrt{5})/2i}$ の場合

(14. 62) は $(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5) = x^5$ となる。

(14. 56) は $\alpha_3^5 = 0$ となる。これより, $(x_1, x_2, x_3, x_4, x_5) = (0, 0, 0, 0, 0)$ となる。

これより, 本例でもべき根の選び方に制約があり, 正しい根が得られるのは(1)の場合だけである。この制約を回避する1つの方法として, ζ_5 を付加した体上で予め $g(x)$ を因数分解しておき, ここから根の計算を始める方法がある。この方法によると, 計算結果は以下となる。

$$g(x) = x^5 + 2160 + 4320\zeta_5 - 1335\zeta_5^2 + 5655\zeta_5^3 \quad (14. 65)$$

$$G_0 = \{\sigma_1, \sigma_7, \sigma_9, \sigma_{16}, \sigma_{19}\}, \quad G_1 = \{\sigma_1\} \quad (14. 66)$$

$$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0, \quad \beta_1^5 - (2160 + 4320\zeta_5 - 1335\zeta_5^2 + 5655\zeta_5^3) = 0 \quad (14. 67)$$

$$x_1 = \beta_1(4 + 3\zeta_5 - 3\zeta_5^2 - 4\zeta_5^3)/5, \quad x_2 = \beta_1(-1 + 3\zeta_5 + 7\zeta_5^2 + 6\zeta_5^3)/5 \quad (14. 68)$$

$$x_3 = \beta_1(-6 - 7\zeta_5 - 3\zeta_5^2 + \zeta_5^3)/5, \quad x_4 = \beta_1(-1 - 7\zeta_5 - 8\zeta_5^2 - 4\zeta_5^3)/5 \quad (14. 69)$$

$$x_5 = \beta_1(4 + 8\zeta_5 + 7\zeta_5^2 + \zeta_5^3)/5 \quad (14. 70)$$

$$(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5) = x^5 - 3 \quad (14. 71)$$

(14. 71) はべき根の選び方に関係なく, 常に $(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5) = x^5 - 3$ となる。

(14. 67) は $\beta_1^5 + 15\sqrt{(375125 - 167761\sqrt{5})/2i} = \beta_1^5 + 3\{\sqrt{(25 - 11\sqrt{5})/2i}\}^5$ となる。

$\beta_1 = -\sqrt[5]{3}\sqrt{(25 - 11\sqrt{5})/2i}$ ならば, $(x_1, x_2, x_3, x_4, x_5) = (X_5, X_2, X_3, X_4, X_1)$ となる。

$\beta_1 = -\sqrt[5]{3}\zeta_5\sqrt{(25 - 11\sqrt{5})/2i}$ ならば, $(x_1, x_2, x_3, x_4, x_5) = (X_1, X_3, X_5, X_4, X_2)$ となる。

$\beta_1 = -\sqrt[5]{3}\zeta_5^2\sqrt{(25 - 11\sqrt{5})/2i}$ ならば, $(x_1, x_2, x_3, x_4, x_5) = (X_2, X_4, X_5, X_1, X_3)$ となる。

$\beta_1 = -\sqrt[5]{3}\zeta_5^3\sqrt{(25 - 11\sqrt{5})/2i}$ ならば, $(x_1, x_2, x_3, x_4, x_5) = (X_3, X_5, X_1, X_2, X_4)$ となる。

$\beta_1 = -\sqrt[5]{3}\zeta_5^4\sqrt{(25 - 11\sqrt{5})/2i}$ ならば, $(x_1, x_2, x_3, x_4, x_5) = (X_4, X_1, X_2, X_3, X_5)$ となる。

この方法によれば, べき根の選び方の制約を回避することができる。

(追記)「ガロア理論に基づいた解法」では, 体の拡大列を一段ずつ登りながら解いていくので, その計算結果(14. 57)-(14. 61)は(14. 64)のような簡潔な式にはならない。(14. 57)-(14. 61)が(14. 64)

と一致することを示したが, $15\sqrt{(375125 + 167761\sqrt{5})/2i}$ から $3\{\sqrt{(25 + 11\sqrt{5})/2i}\}^5$ への書き換えを要するなど, 決して容易ではなかったことを付記しておく。

15. 可解な5次方程式の解法

以下の可解な5次方程式の解法を示す。ただし、 x^4 の項は消去し、係数 a_3, a_2, a_1, a_0 は有理数とする。

$$f(x)=x^5+a_3x^3+a_2x^2+a_1x+a_0=0 \quad (15.1)$$

その根 x_1, x_2, x_3, x_4, x_5 を次式で表す。 ζ_5 は1の原始5乗根である。

$$\begin{aligned} x_1 &= A+B+C+D, \quad x_2 = \zeta_5 A + \zeta_5^2 B + \zeta_5^3 C + \zeta_5^4 D, \quad x_3 = \zeta_5^2 A + \zeta_5^4 B + \zeta_5 C + \zeta_5^3 D \\ x_4 &= \zeta_5^3 A + \zeta_5 B + \zeta_5^4 C + \zeta_5^2 D, \quad x_5 = \zeta_5^4 A + \zeta_5^3 B + \zeta_5^2 C + \zeta_5 D \end{aligned} \quad (15.2)$$

これを $f(x)=(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)$ に代入して展開すると、 A, B, C, D と a_3, a_2, a_1, a_0 の関係式として、次式が得られる。

$$-5(AD+BC)=a_3 \quad (15.3)$$

$$-5(A^2C+AB^2+BD^2+C^2D)=a_2 \quad (15.4)$$

$$-5(A^3B+AC^3+B^3D+CD^3-A^2D^2-B^2C^2+ABCD)=a_1 \quad (15.5)$$

$$-(A^5+B^5+C^5+D^5)+5(AD-BC)(A^2C-AB^2+BD^2-C^2D)=a_0 \quad (15.6)$$

この連立方程式を解けば A, B, C, D が求められるが、一般の5次方程式は解けないので、この連立方程式も解けない。ところが、可解な5次方程式の場合は、以下の α, β が有理数となり、しかもその値を知ることができる。

$$\{25(AD-BC)\}^2=\alpha \quad (15.7)$$

$$\{125(A^2C-AB^2+BD^2-C^2D)\}^2=\beta \quad (15.8)$$

このとき、(15.3), (15.4), (15.7), (15.8)からなる連立方程式を解けば A, B, C, D が求められる。まず、(15.2)を A, B, C, D について解く。

$$\begin{aligned} A &= (x_1 + \zeta_5^4 x_2 + \zeta_5^3 x_3 + \zeta_5^2 x_4 + \zeta_5 x_5) / 5, \quad B = (x_1 + \zeta_5^3 x_2 + \zeta_5 x_3 + \zeta_5^4 x_4 + \zeta_5^2 x_5) / 5 \\ C &= (x_1 + \zeta_5^2 x_2 + \zeta_5^4 x_3 + \zeta_5 x_4 + \zeta_5^3 x_5) / 5, \quad D = (x_1 + \zeta_5 x_2 + \zeta_5^2 x_3 + \zeta_5^3 x_4 + \zeta_5^4 x_5) / 5 \end{aligned} \quad (15.9)$$

これを(15.7)の左辺に代入すると、 α が x_1, x_2, x_3, x_4, x_5 の多項式で表される。ただし、長い式になるので省略する。これを $\alpha(x_1, x_2, x_3, x_4, x_5)$ と表記すると、その値は有理数ではあるが、 x_1, x_2, x_3, x_4, x_5 の対称式ではない。ここで、 x_1, x_2, x_3, x_4, x_5 に $5!=120$ 通りの置換を作用させると、 $\alpha(x_1, x_2, x_3, x_4, x_5)$ はすべて異なる式になるのではなく、 $\alpha(x_1, x_2, x_3, x_4, x_5)$ と同じ式が20個、 $\alpha(x_1, x_2, x_3, x_5, x_4)$ と同じ式が20個、 $\alpha(x_1, x_2, x_4, x_3, x_5)$ と同じ式が20個、 $\alpha(x_1, x_2, x_4, x_5, x_3)$ と同じ式が20個、 $\alpha(x_1, x_2, x_5, x_3, x_4)$ と同じ式が20個、 $\alpha(x_1, x_2, x_5, x_4, x_3)$ と同じ式が20個となる。ここで

$$\begin{aligned} f_\alpha(x) &= (x - \alpha(x_1, x_2, x_3, x_4, x_5)) (x - \alpha(x_1, x_2, x_3, x_5, x_4)) (x - \alpha(x_1, x_2, x_4, x_3, x_5)) \\ &\quad \times (x - \alpha(x_1, x_2, x_4, x_5, x_3)) (x - \alpha(x_1, x_2, x_5, x_3, x_4)) (x - \alpha(x_1, x_2, x_5, x_4, x_3)) \end{aligned} \quad (15.10)$$

とすると、これは x_1, x_2, x_3, x_4, x_5 の対称式であるから、その係数は a_3, a_2, a_1, a_0 で表され、しかもその根のうちの1つは α である。上式を展開して、係数を a_3, a_2, a_1, a_0 で表すと次式となる。

$$\begin{aligned} f_\alpha(x) &= x^6 - 10(20a_1 + 3a_3^2)x^5 + 25(880a_1^2 - 800a_0a_2 + 32a_2^2a_3 + 104a_1a_3^2 + 15a_3^4)x^4 - 500(2240a_1^3 - 3200a_0a_1a_2 + 32a_2^4 \\ &\quad - 2000a_0^2a_3 + 48a_1a_2^2a_3 + 368a_1^2a_3^2 - 560a_0a_2a_3^2 + 32a_2^2a_3^3 + 4a_1a_3^4 + 5a_3^6)x^3 + 625(44800a_1^4 - 128000a_0a_1^2a_2 \\ &\quad + 160000a_0^2a_2^2 + 2560a_1a_2^4 - 160000a_0^2a_1a_3 - 1280a_1^2a_2^2a_3 - 12800a_0a_2^3a_3 + 1280a_1^3a_3^2 + 19200a_0a_1a_2a_3^2 + 640a_2^4a_3^2 \\ &\quad - 24000a_0^2a_3^3 - 960a_1a_2^2a_3^3 + 1440a_1^2a_3^4 - 1920a_0a_2a_3^4 + 192a_2^2a_3^5 - 176a_1a_3^6 + 15a_3^8)x^2 - 6250(1600000a_0^4 + 54272a_1^5 \\ &\quad - 307200a_0a_1^3a_2 + 512000a_0^2a_1a_2^2 + 1536a_1^2a_2^4 + 29696a_0a_2^5 + 64000a_0^2a_1^2a_3 - 320000a_0^3a_2a_3 + 14848a_1^3a_2^2a_3 \\ &\quad - 207360a_0a_1a_2^3a_3 + 1024a_2^6a_3 - 20736a_1^4a_3^2 + 222720a_0a_1^2a_2a_3^2 + 326400a_0^2a_2^2a_3^2 - 4096a_1a_2^4a_3^2 - 428800a_0^2a_1a_3^3 \\ &\quad + 6400a_1^2a_2^2a_3^3 + 3072a_0a_2^3a_3^3 - 896a_1^3a_3^4 - 21504a_0a_1a_2a_3^4 + 448a_2^4a_3^4 + 43296a_0^2a_3^5 - 1248a_1a_2^2a_3^5 + 992a_1^2a_3^6 \\ &\quad - 160a_0a_2a_3^6 + 64a_2^2a_3^7 - 92a_1a_3^8 + 3a_3^{10})x + 15625(320a_1^3 - 1600a_0a_1a_2 - 64a_2^4 + 4000a_0^2a_3 + 224a_1a_2^2a_3 - 176a_1^2a_3^2 \\ &\quad - 80a_0a_2a_3^2 - 16a_2^2a_3^3 + 28a_1a_3^4 - a_3^6) \end{aligned} \quad (15.11)$$

同様に, β については次式となる。

$$\begin{aligned}
f_\beta(x) = & x^6 - 250(3a_2^2 - 8a_1a_3)x^5 - 15625(128a_1^3 - 480a_0a_1a_2 - 15a_2^4 + 800a_0^2a_3 + 80a_1a_2^2a_3 - 96a_1^2a_3^2 - 32a_0a_2a_3^2)x^4 \\
& + 7812500(-800a_0^2a_1^2 + 2000a_0^3a_2 + 96a_1^3a_2^2 - 336a_0a_1a_2^3 - 5a_2^6 - 256a_1^4a_3 + 864a_0a_1^2a_2a_3 + 560a_0^2a_2^2a_3 + 40a_1a_2^4a_3 \\
& - 1280a_0^2a_1a_3^2 - 96a_1^2a_2^2a_3^2 - 32a_0a_2^3a_3^2 + 64a_1^3a_3^3 + 96a_0a_1a_2a_3^3 - 32a_0^2a_3^4)x^3 + 244140625(4096a_1^6 - 30720a_0a_1^4a_2 \\
& + 67200a_0^2a_1^2a_2^2 - 24000a_0^3a_2^3 - 384a_1^3a_2^4 + 1152a_0a_1a_2^5 + 15a_2^8 + 25600a_0^2a_1^3a_3 - 128000a_0^3a_1a_2a_3 + 2048a_1^4a_2^2a_3 \\
& - 5760a_0a_1^2a_2^3a_3 - 1920a_0^2a_2^4a_3 - 160a_1a_2^6a_3 + 160000a_0^4a_3^2 - 2048a_1^5a_3^2 + 2560a_0a_1^3a_2a_3^2 + 15360a_0^2a_1a_2^2a_3^2 \\
& + 576a_1^2a_2^4a_3^2 + 192a_0a_2^5a_3^2 - 2560a_0^2a_1^2a_3^3 - 12800a_0^3a_2a_3^3 - 768a_1^3a_2^2a_3^3 - 1152a_0a_1a_2^3a_3^3 + 256a_1^4a_3^4 + 1536a_0a_1^2a_2a_3^4 \\
& + 640a_0^2a_2^2a_3^4 - 1024a_0^2a_1a_3^5)x^2 - 61035156250(1600000a_0^6 + 28672a_0^2a_1^5 - 179200a_0^3a_1^3a_2 + 192000a_0^4a_1a_2^2 \\
& + 3072a_0a_1^4a_2^3 - 20544a_0^2a_1^2a_2^4 + 43296a_0^3a_2^5 - 64a_1^3a_2^6 + 96a_0a_1a_2^7 + 3a_2^{10} + 384000a_0^4a_1^2a_3 - 320000a_0^5a_2a_3 \\
& - 12288a_0a_1^5a_2a_3 + 89088a_0^2a_1^3a_2^2a_3 - 220160a_0^3a_1a_2^3a_3 + 512a_1^4a_2^4a_3 - 576a_0a_1^2a_2^5a_3 - 160a_0^2a_2^6a_3 - 40a_1a_2^8a_3 \\
& + 1024a_0^2a_1^4a_3^2 + 17920a_0^3a_1^2a_2a_3^2 + 326400a_0^4a_2^2a_3^2 - 1024a_1^5a_2^2a_3^2 - 1024a_0a_1^3a_2^3a_3^2 + 3072a_0^2a_1a_2^4a_3^2 + 192a_1^2a_2^6a_3^2 \\
& + 64a_0a_2^7a_3^2 - 204800a_0^4a_1a_3^3 + 7168a_0a_1^4a_2a_3^3 - 9216a_0^2a_1^2a_2^2a_3^3 + 3072a_0^3a_2^3a_3^3 - 384a_1^3a_2^4a_3^3 - 576a_0a_1a_2^5a_3^3 \\
& - 6144a_0^2a_1^3a_3^4 - 6144a_0^3a_1a_2a_3^4 + 256a_1^4a_2^2a_3^4 + 1536a_0a_1^2a_2^3a_3^4 + 448a_0^2a_2^4a_3^4 + 29696a_0^4a_3^5 - 1024a_0a_1^3a_2a_3^5 \\
& - 2048a_0^2a_1a_2^2a_3^5 + 1024a_0^2a_1^2a_3^6 + 1024a_0^3a_2a_3^6)x + 3814697265625(-1600a_0^2a_1^2 + 4000a_0^3a_2 + 48a_0a_1a_2^3 - a_2^6 \\
& - 192a_0a_1^2a_2a_3 - 80a_0^2a_2^2a_3 + 8a_1a_2^4a_3 + 640a_0^2a_1a_3^2 - 16a_1^2a_2^2a_3^2 - 16a_0a_2^3a_3^2 + 64a_0a_1a_2a_3^3 - 64a_0^2a_3^4)^2 \quad (15.12)
\end{aligned}$$

ここで, a_3, a_2, a_1, a_0 は有理数としたので, $f_\alpha(x), f_\beta(x)$ の係数も有理数となる。このとき, 有理根 α, β は $f_\alpha(x), f_\beta(x)$ の定数項の約数のうちのどれかであって, それらは必ず求めることができる。ちなみに, $f(x)$ が可解であることと, $f_\alpha(x), f_\beta(x)$ に有理根が存在することは同値であることが知られている。 $f(x)$ の可解性を調べるには, ガロア群を調べるよりも, $f_\alpha(x), f_\beta(x)$ の有理根の有無を調べるほうが容易である。つぎに, (15.3), (15.4), (15.5), (15.6)からなる連立方程式の代わりに, (15.3), (15.4), (15.7), (15.8)からなる連立方程式を解いて A, B, C, D を求める。この A, B, C, D は(15.2)に代入して, 根 x_1, x_2, x_3, x_4, x_5 を求めるのに使うだけであるから, 任意の1組の A, B, C, D だけを求めれば十分である。まず, (15.3), (15.7)より次式を得る。

$$AD = -(a_3 + b_3)/10, \quad BC = -(a_3 - b_3)/10, \quad b_3 = \sqrt{\alpha}/5 \quad (15.13)$$

(15.4), (15.8)より次式を得る。

$$A^2C + BD^2 = -(a_2 + b_2)/10, \quad AB^2 + C^2D = -(a_2 - b_2)/10, \quad b_2 = \sqrt{\beta}/25 \quad (15.14)$$

(15.13)より $(A^2C)(BD^2) = -(a_3 + b_3)^2(a_3 - b_3)/1000$, これと(15.14)の第1式より次式を得る。

$$\begin{aligned}
A^2C &= -(a_2 + b_2 + \sqrt{r_1})/20, \quad BD^2 = -(a_2 - b_2 - \sqrt{r_1})/20 \\
r_1 &= (a_2 + b_2)^2 + 2(a_3 + b_3)^2(a_3 - b_3)/5 \quad (15.15)
\end{aligned}$$

(15.13)より $(AB^2)(C^2D) = -(a_3 + b_3)(a_3 - b_3)^2/1000$, これと(15.14)の第2式より次式を得る。

$$\begin{aligned}
AB^2 &= -(a_2 - b_2 + \sqrt{r_2})/20, \quad C^2D = -(a_2 - b_2 - \sqrt{r_2})/20 \\
r_2 &= (a_2 - b_2)^2 + 2(a_3 + b_3)(a_3 - b_3)^2/5 \quad (15.16)
\end{aligned}$$

これより後は5つの場合に分けて考える。

(1) $a_3^2 - b_3^2 \neq 0$ の場合

A^5, B^5, C^5, D^5 は次式となる。

$$\begin{aligned}
A^5 &= (A^2C)^2(AB^2)/(BC)^2 \\
&= [- (a_2 - b_2) \{ (a_2 + b_2)^2 + r_1 \} - 2(a_2^2 - b_2^2) \sqrt{r_1} - \{ (a_2 + b_2)^2 + r_1 \} \sqrt{r_2} - 2(a_2 + b_2) \sqrt{r_1} \sqrt{r_2}] / 80(a_3 - b_3)^2 \\
&= p + q \pm \sqrt{(a_3 + b_3)^5/10^5 + (p + q)^2} \quad (15.17)
\end{aligned}$$

$$\begin{aligned}
B^5 &= (AB^2)^2(BD^2)/(AD)^2 \\
&= [- (a_2 + b_2) \{ (a_2 - b_2)^2 + r_2 \} - 2(a_2^2 - b_2^2) \sqrt{r_2} + \{ (a_2 - b_2)^2 + r_2 \} \sqrt{r_1} + 2(a_2 - b_2) \sqrt{r_1} \sqrt{r_2}] / 80(a_3 + b_3)^2 \\
&= p - q \pm \sqrt{(a_3 - b_3)^5/10^5 + (p - q)^2} \quad (15.18)
\end{aligned}$$

$$\begin{aligned}
C^5 &= (C^2 D)^2 (A^2 C) / (AD)^2 \\
&= [- (a_2 + b_2) \{ (a_2 - b_2)^2 + r_2 \} + 2 (a_2^2 - b_2^2) \sqrt{r_2} - \{ (a_2 - b_2)^2 + r_2 \} \sqrt{r_1} + 2 (a_2 - b_2) \sqrt{r_1} \sqrt{r_2}] / 80 (a_3 + b_3)^2 \\
&= p - q \mp \sqrt{(a_3 - b_3)^5 / 10^5 + (p - q)^2} \quad (15.19)
\end{aligned}$$

$$\begin{aligned}
D^5 &= (BD^2)^2 (C^2 D) / (BC)^2 \\
&= [- (a_2 - b_2) \{ (a_2 + b_2)^2 + r_1 \} + 2 (a_2^2 - b_2^2) \sqrt{r_1} + \{ (a_2 + b_2)^2 + r_1 \} \sqrt{r_2} - 2 (a_2 + b_2) \sqrt{r_1} \sqrt{r_2}] / 80 (a_3 - b_3)^2 \\
&= p + q \mp \sqrt{(a_3 + b_3)^5 / 10^5 + (p + q)^2} \quad (15.20)
\end{aligned}$$

ここで

$$\begin{aligned}
p &= (A^5 + B^5 + C^5 + D^5) / 4 \\
&= \{-5 (a_2^2 - b_2^2) (a_2 a_3^2 + 2 a_3 b_2 b_3 + a_2 b_3^2) - (a_3^2 - b_3^2) (a_2 a_3^3 - 3 a_3^2 b_2 b_3 + 3 a_2 a_3 b_3^2 - b_2 b_3^3) \\
&\quad - 5 (a_3^2 b_2 + 2 a_2 a_3 b_3 + b_2 b_3^2) \sqrt{r_1} \sqrt{r_2}\} / 200 (a_3^2 - b_3^2)^2 \quad (15.21)
\end{aligned}$$

$$\begin{aligned}
q &= (A^5 - B^5 - C^5 + D^5) / 4 \\
&= \{-5 (a_2^2 - b_2^2) (a_3^2 b_2 + 2 a_2 a_3 b_3 + b_2 b_3^2) + (a_3^2 - b_3^2) (a_3^3 b_2 - 3 a_2 a_3^2 b_3 + 3 a_3 b_2 b_3^2 - a_2 b_3^3) \\
&\quad - 5 (a_2 a_3^2 + 2 a_3 b_2 b_3 + a_2 b_3^2) \sqrt{r_1} \sqrt{r_2}\} / 200 (a_3^2 - b_3^2)^2 \quad (15.22)
\end{aligned}$$

A^5, D^5 の両式において、第4辺の複号は一方が正、他方が負であって、それは第4辺が第3辺と等しくなるように決められる。 B^5, C^5 についても同様である。つぎに、 A^5, B^5, C^5, D^5 の5乗根より A, B, C, D を決める。 A は A^5 の5乗根のうち、任意の1つを選ぶ。 D は D^5 の5乗根のうち、(15.13)の第1式を満たすものを選ぶ。 C は C^5 の5乗根のうち、(15.15)の第1式を満たすものを選ぶ。 B は B^5 の5乗根のうち、(15.13)の第2式を満たすものを選ぶ。ここで解いたのは(15.3), (15.4), (15.7), (15.8)からなる連立方程式であるが、本来解くべきものは(15.3), (15.4), (15.5), (15.6)からなる連立方程式である。最後に、この A, B, C, D が(15.5), (15.6)を満たしていることを次式で確認する。

$$a_1 = (a_3^2 + 3b_3^2) / 20 + \{a_3 (a_2^2 - b_2^2) + b_3 \sqrt{r_1} \sqrt{r_2}\} / 2 (a_3^2 - b_3^2) \quad (15.23)$$

$$a_0 = -(A^5 + B^5 + C^5 + D^5) + b_2 b_3 / 5 \quad (15.24)$$

(例1) $f(x) = x^5 + 2x^3 + 4x^2 - x + 4$ の場合

$$a_3 = 2, a_2 = 4, a_1 = -1, a_0 = 4$$

$$\begin{aligned}
f_\alpha(x) &= x^6 + 80x^5 - 276800x^4 + 19200000x^3 + 20590080000x^2 - 5015756800000x + 230068224000000 \\
&= (x - 360) (x^5 + 440x^4 - 118400x^3 - 23424000x^2 + 12157440000x - 639078400000)
\end{aligned}$$

$$\alpha = 360, b_3 = 6\sqrt{10}/5, AD = -(5 + 3\sqrt{10})/25, BC = -(5 - 3\sqrt{10})/25$$

$$\begin{aligned}
f_\beta(x) &= x^6 - 16000x^5 - 3800000000x^4 + 6864000000000x^3 + 22788000000000000x^2 \\
&\quad - 8591680000000000000000000x + 27423360000000000000000000 \\
&= (x - 4000) (x^5 - 12000x^4 - 4280000000x^3 + 5152000000000x^2 + 4339600000000000000x \\
&\quad - 6855840000000000000000000)
\end{aligned}$$

$$\beta = 4000, b_2 = 4\sqrt{10}/5, r_1 = 176(10 + \sqrt{10})/125, r_2 = 176(10 - \sqrt{10})/125$$

$$A^2 C = \{(5 + \sqrt{10})/25 + \sqrt{55(10 + \sqrt{10})/125}\}, BD^2 = -\{(5 + \sqrt{10})/25 - \sqrt{55(10 + \sqrt{10})/125}\}$$

$$AB^2 = -\{(5 - \sqrt{10})/25 + \sqrt{55(10 - \sqrt{10})/125}\}, C^2 D = -\{(5 - \sqrt{10})/25 - \sqrt{55(10 - \sqrt{10})/125}\}$$

$$p = -13/25, q = -4\sqrt{10}/25$$

$$A^5 = -(13 + 4\sqrt{10})/25 - 6(23 + 6\sqrt{10})\sqrt{55(10 + \sqrt{10})}/21125$$

$$-(10215 + 3113\sqrt{10})\sqrt{55(10 - \sqrt{10})}/528125$$

$$= -(13 + 4\sqrt{10})/25 - \sqrt{11(19850 + 6277\sqrt{10})}/625 \quad (\text{近似値}-2.08329 \text{より複号は負})$$

$$\begin{aligned}
B^5 &= -(13-4\sqrt{10})/25-6(23-6\sqrt{10})\sqrt{55(10-\sqrt{10})}/21125 \\
&\quad + (10215-3113\sqrt{10})\sqrt{55(10+\sqrt{10})}/528125 \\
&= -(13-4\sqrt{10})/25-\sqrt{11(19850-6277\sqrt{10})}/625 \quad (\text{近似値}-0.0173202 \text{より複号は負}) \\
C^5 &= -(13-4\sqrt{10})/25+6(23-6\sqrt{10})\sqrt{55(10-\sqrt{10})}/21125 \\
&\quad - (10215-3113\sqrt{10})\sqrt{55(10+\sqrt{10})}/528125 \\
&= -(13-4\sqrt{10})/25+\sqrt{11(19850-6277\sqrt{10})}/625 \quad (\text{近似値}-0.0107509 \text{より複号は正}) \\
D^5 &= -(13+4\sqrt{10})/25+6(23+6\sqrt{10})\sqrt{55(10+\sqrt{10})}/21125 \\
&\quad + (10215+3113\sqrt{10})\sqrt{55(10-\sqrt{10})}/528125 \\
&= -(13+4\sqrt{10})/25+\sqrt{11(19850+6277\sqrt{10})}/625 \quad (\text{近似値}0.031363 \text{より複号は正})
\end{aligned}$$

A, B, C, D は各々 A^5, B^5, C^5, D^5 の実数の5乗根を選ぶ。この A, B, C, D は(15. 23), (15. 24)を満たしている。

(2) $a_3^2-b_3^2=0, a_2^2-b_2^2 \neq 0$ の場合

これは A, B, C, D のうちの1つが0の場合である。 $D=0$ とすると, (15. 3), (15. 14)より次式を得る。

$$BC=-a_3/5, A^2C=-(a_2+b_2)/10, AB^2=-(a_2-b_2)/10 \quad (15. 25)$$

A^5, B^5, C^5, D^5 は次式となる。

$$A^5=(A^2C)^2(AB^2)/(BC)^2=-(a_2+b_2)^2(a_2-b_2)/40a_3^2 \quad (15. 26)$$

$$B^5=(AB^2)^2(BC)/(A^2C)=a_3(a_2-b_2)^2/50(a_2+b_2) \quad (15. 27)$$

$$C^5=(A^2C)(BC)^4/(AB^2)^2=-2a_3^4(a_2+b_2)/125(a_2-b_2)^2 \quad (15. 28)$$

$$D^5=0 \quad (15. 29)$$

つぎに, A^5, B^5, C^5 の5乗根より A, B, C を決める。 A は A^5 の5乗根のうち, 任意の1つを選ぶ。 C は C^5 の5乗根のうち, (15. 25)の第2式を満たすものを選ぶ。 B は B^5 の5乗根のうち, (15. 25)の第1式を満たすものを選ぶ。この A, B, C が(15. 5), (15. 6)を満たしていることを次式で確認する。

$$a_1=(a_2^2-b_2^2)/4a_3-a_3^2(a_2+b_2)/5(a_2-b_2)+a_3^2/5 \quad (15. 30)$$

$$a_0=-(A^5+B^5+C^5)-a_3b_2/5 \quad (15. 31)$$

(例2) $f(x)=x^5+10x^3+20x^2+10x+6$ の場合

$$a_3=10, a_2=20, a_1=10, a_0=6$$

$$\begin{aligned}
f_\alpha(x) &= x^6-5000x^5+9350000x^4-9940000000x^3+7877500000000x^2-6485860000000000x \\
&\quad +1199025000000000000 \\
&= (x-2500)(x^5-2500x^4+3100000x^3-21900000000x^2+2402500000000x-479610000000000)
\end{aligned}$$

$$\alpha=2500, b_3=10, BC=-2$$

$$\begin{aligned}
f_\beta(x) &= x^6-100000x^5+11000000000x^4-42500000000000x^3+1806250000000000000x^2 \\
&\quad -1086806250000000000000000x \\
&= x(x^5-100000x^4+11000000000x^3-42500000000000x^2+1806250000000000000x \\
&\quad -1086806250000000000000000)
\end{aligned}$$

$$\beta=0, b_2=0, A^2C=-2, AB^2=-2$$

$$A^5=-2, B^5=4, C^5=-8, D=0$$

A, B, C は各々 A^5, B^5, C^5 の実数の5乗根を選ぶ。この A, B, C は(15. 30), (15. 31)を満たしている。

(3) $a_3^2 - b_3^2 = 0$, $a_2^2 - b_2^2 = 0$, $a_3 \neq 0$ の場合

これは $A=D=0$ または $B=C=0$ の場合である。 $B=C=0$ とすると, (15. 3), (15. 6) より次式を得る。

$$AD = -a_3/5, A^5 + D^5 = -a_0 \quad (15. 32)$$

A^5, B^5, C^5, D^5 は次式となる。

$$A^5 = -a_0/2 + \sqrt{(a_0/2)^2 + (a_3/5)^5}, B^5 = C^5 = 0, D^5 = -a_0/2 - \sqrt{(a_0/2)^2 + (a_3/5)^5} \quad (15. 33)$$

つぎに, A^5, D^5 の5乗根より A, D を決める。 A は A^5 の5乗根のうち, 任意の1つを選ぶ。 D は D^5 の5乗根のうち, (15. 32) の第1式を満たすものを選ぶ。 この A, D が (15. 4), (15. 5) を満たしていることを次式で確認する。

$$a_2 = 0 \quad (15. 34)$$

$$a_1 = a_3^2/5 \quad (15. 35)$$

(例3) $f(x) = x^5 + 5x^3 + 5x + 2$ の場合

$$a_3 = 5, a_2 = 0, a_1 = 5, a_0 = 2$$

$$f_\alpha(x) = x^6 - 1750x^5 + 1109375x^4 - 280312500x^3 + 11630859375x^2 + 2878066406250x + 104742431640625 \\ = (x - 625)(x^5 - 1125x^4 + 406250x^3 - 26406250x^2 - 4873046875x - 167587890625)$$

$$\alpha = 625, b_3 = 5, AD = -1$$

$$f_\beta(x) = x^6 + 50000x^5 + 437500000x^4 - 4687500000000x^3 + 8789062500000000x^2 \\ - 25000000000000000000x \\ = x(x^5 + 50000x^4 + 437500000x^3 - 4687500000000x^2 + 8789062500000000x - 2500000000000000000)$$

$$\beta = 0, b_2 = 0, A^5 + D^5 = -2$$

$$A^5 = -1 + \sqrt{2}, B = C = 0, D^5 = -1 - \sqrt{2}$$

A, D は各々 A^5, D^5 の実数の5乗根を選ぶ。 この A, D は (15. 34), (15. 35) を満たしている。

(4) $a_3^2 - b_3^2 = 0$, $a_2^2 - b_2^2 = 0$, $a_3 = 0$, $a_2 \neq 0$ の場合

これは $A=B=0$, $A=C=0$, $B=D=0$, $C=D=0$ のうちのどれかの場合である。 $C=D=0$ とすると, (15. 4), (15. 5) より次式を得る。

$$AB^2 = -a_2/5, A^3B = -a_1/5 \quad (15. 36)$$

A^5, B^5, C^5, D^5 は次式となる。

$$A^5 = (A^3B)^2/(AB^2) = -a_1^2/5a_2, B^5 = (AB^2)^3/(A^3B) = a_2^3/25a_1, C^5 = D^5 = 0 \quad (15. 37)$$

つぎに, A^5, B^5 の5乗根より A, B を決める。 A は A^5 の5乗根のうち, 任意の1つを選ぶ。 B は B^5 の5乗根のうち, (15. 36) の第2式を満たすものを選ぶ。 この A, B は (15. 3) を既に満たしている。 (15. 6) を満たしていることを次式で確認する。

$$a_0 = -A^5 - B^5 \quad (15. 38)$$

(例4) $f(x) = x^5 - 10x^2 + 10x + 2$ の場合

$$a_3 = 0, a_2 = -10, a_1 = 10, a_0 = 2$$

$$f_\alpha(x) = x^6 - 2000x^5 + 2600000x^4 - 1600000000x^3 + 640000000000x^2 - 57760000000000x \\ = x(x^5 - 2000x^4 + 2600000x^3 - 1600000000x^2 + 640000000000x - 5776000000000)$$

$$\alpha = 0, b_3 = 0$$

$$f_\beta(x) = x^6 - 75000x^5 - 1156250000x^4 + 84687500000000x^3 + 2069335937500000000x^2 \\ + 12358007812500000000000x + 325256347656250000000000 \\ = (x - 62500)(x^5 - 12500x^4 - 1937500000x^3 - 36406250000000x^2 - 206054687500000000x - 52041015625000000000)$$

$$\beta = 62500, b_2 = 10, AB^2 = 2, A^3B = -2$$

$$A^5=2, B^5=-4, C^5=0, D^5=0$$

A, B は各々 A^5, B^5 の実数の5乗根を選ぶ。この A, B は(15.38)を満たしている。

$$(5) a_3^2 - b_3^2 = 0, a_2^2 - b_2^2 = 0, a_3 = 0, a_2 = 0 \text{ の場合}$$

これは A, B, C, D のうちの3つが0の場合である。 $B=C=D=0$ とすると、(15.6)より次式を得る。

$$A^5 = -a_0, B^5 = C^5 = D^5 = 0 \quad (15.39)$$

A は A^5 の5乗根のうち、任意の1つを選ぶ。この A は(15.3), (15.4)を既に満たしている。(15.5)を満たしていることを次式で確認する。

$$a_1 = 0 \quad (15.40)$$

《可解な5次方程式の一覧表》

参考文献(7)には、 a_3, a_2, a_1, a_0 が整数で $-12 \leq a_3, a_2, a_1 \leq 12, 1 \leq a_0 \leq 12$ のとき、既約で可解な5次方程式の一覧表が付いていた。現在は削除されているので、以下にその一覧表を示す。

a_3	a_2	a_1	a_0
-12	-7	10	4
-11	-11	11	11
-11	-10	11	10
-11	-6	10	4
-11	11	6	1
-10	5	10	1
-10	10	5	2
-9	-4	10	4
-9	9	4	3
-9	12	-6	12
-8	-3	10	4
-8	8	3	4
-7	7	2	5
-7	10	-5	2
-6	-1	10	4
-6	6	1	6
-6	12	-9	12
-5	0	5	3
-5	0	5	4
-5	0	5	5
-5	0	5	6
-5	0	5	7
-5	0	5	8
-5	0	5	9
-5	0	5	10
-5	0	5	11
-5	0	5	12
-5	0	10	4
-5	0	10	9
-5	5	0	7
-5	7	8	5
-5	10	-10	8

a_3	a_2	a_1	a_0
-5	11	-3	9
-4	1	10	4
-4	4	-1	8
-3	-4	8	1
-3	1	7	5
-3	2	6	3
-3	2	10	4
-3	3	-2	9
-3	11	-3	3
-2	2	-3	10
-2	3	10	4
-2	7	-12	7
-2	9	-2	3
-1	-10	8	9
-1	-7	1	11
-1	-4	7	2
-1	-2	3	4
-1	1	-4	11
-1	2	-2	1
-1	4	4	1
-1	4	10	4
-1	7	-1	3
0	-10	10	2
0	-3	2	1
0	0	-5	12
0	0	0	2
0	0	0	3
0	0	0	4
0	0	0	5
0	0	0	6
0	0	0	7
0	0	0	8

a_3	a_2	a_1	a_0
0	0	0	9
0	0	0	10
0	0	0	11
0	0	0	12
0	5	-5	8
0	5	-4	1
0	5	0	3
0	5	10	4
0	10	-10	6
1	2	12	9
1	3	1	3
1	6	4	3
1	6	10	4
1	10	-12	8
2	1	2	3
2	4	-1	4
2	5	-4	4
2	7	10	4
2	8	9	8
3	-1	3	3
3	6	-1	4
3	8	6	9
3	8	10	4
4	-3	4	3
4	4	8	8
4	5	12	4
4	9	10	1
4	9	10	4
5	-5	5	3
5	0	5	1
5	0	5	2
5	0	5	3

a_3	a_2	a_1	a_0
5	0	5	4
5	0	5	5
5	0	5	6
5	0	5	7
5	0	5	8
5	0	5	9
5	0	5	10
5	0	5	12
5	1	9	5
5	10	0	5
5	10	5	4
5	10	10	4
6	-7	6	3
6	4	-9	4
6	5	12	3
6	11	10	4
7	-9	7	3
7	3	5	5
7	5	5	1
7	5	9	5
7	10	-6	5
7	12	10	4
8	-11	8	3
8	2	2	2
8	5	6	7
9	5	3	9
10	0	0	5
10	5	0	11
10	10	10	3
10	12	-11	4
11	-2	0	7
11	-2	4	8

参考文献

- (1) 五次元世界の冒険, 井汲景太, <http://ikumi.que.jp/blog/archives/21>
- (2) Maximaで綴る数学の旅, jurupapa
<http://maxima.hatenablog.jp/archive/category/%E6%95%B0%E5%AD%A6>
- (3) 可解な5次方程式について, 大迎規宏
<http://repository.hyogo-u.ac.jp/dspace/bitstream/10132/1612/1/ZD30301003.pdf>
- (4) 数学が育っていく物語5 方程式, 志賀浩二, 岩波書店
- (5) 代数方程式とガロア理論, 中島匠一, 共立出版
- (6) ガロア理論の頂を踏む, 石井俊全, ベレ出版
- (7) 5次方程式の可解性の高速判定法, 元吉文男
<http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/0848-01.pdf>