

# F1, F2 を求める with Mathematica14.0

## §1. F35とガロア群

```
In[*]:= ClearAll["`*"]
```

既約で有理数係数かつ monic な7次方程式

「 $f = x^7 + a_1 x^6 + a_2 x^5 + a_3 x^4 + a_4 x^3 + a_5 x^2 + a_6 x + a_7 = 0$ 」の解を  $x_0, x_1, \dots, x_6$  とします.  $x_0 \sim x_6$  から異なる3つの解  $x_i, x_j, x_k$  ( $0 \leq i < j < k \leq 6$ ) を選んでその和  $s_{ijk}$  を作ります. この時,  $f$  の補助方程式  $F_{35}$  とその係数  $A_i$  を次の様に定義します.

$$\begin{aligned} F_{35} &= (x - s_{012})(x - s_{013}) \cdots (x - s_{456}) = \\ &= \prod_{0 \leq i < j < k \leq 6} (x - s_{ijk}) = x^{35} + A_1 x^{34} + A_2 x^{33} + \cdots + A_{34} x + A_{35} \end{aligned}$$

F35の式は下のclosed cellに入っています(↓). 求め方は F35.nb をご覧ください.

$f$  の解の変換「 $\sigma : x_k \rightarrow x_{k+1}$ 」と「 $\tau : x_k \rightarrow x_{5-k}$ 」を考えます.  
( $k = 0, 1, 2, \dots, 6$ , 添え数字はMod7で考えます)

$f$  のガロア群を  $\text{Gal}$  とすると, 可解な  $\text{Gal}$  は  $F_{42} = \langle \sigma, \tau \rangle, F_{21} = \langle \sigma, \tau^2 \rangle, D_7 = \langle \sigma, \tau^3 \rangle, C_7 = \langle \sigma \rangle$  の4通りです. 位数はそれぞれ 42, 21, 14, 7 です.

原論文によると,  $f$  が既約の時,  $\text{Gal}$  と  $F_{35}$  の有理数体上の因数分解について「Bruen et al」という方が次の発表をされました(1986年) この証明は原論文には載っていません. そのReferenceをご覧ください.

#1	$F_{35}$ が有理数体上で因数分解できない	$\rightarrow \text{Gal} = S_7$ または $A_7$
	$F_{35}$ が $(7+28)$ 次の式に因数分解できる	$\rightarrow \text{Gal}$ の位数は 168
	$F_{35}$ が $(14+21)$ 次の式に因数分解できる	$\rightarrow \text{Gal} = F_{42}$
	$F_{35}$ が $(7+7+21)$ 次の式に因数分解できる	$\rightarrow \text{Gal} = F_{21}$
	$F_{35}$ が $(7+7+7+14)$ 次の式に因数分解できる	$\rightarrow \text{Gal} = D_7$
	$F_{35}$ が $(7+7+7+7+7)$ 次の式に因数分解できる	$\rightarrow \text{Gal} = C_7$

Mathematica では例えば次の様にプログラムできます.

In[239]:=

```
galoisGroup[f0_]:=Module[{f,delta,numbers,factors},
  delta=Coefficient[f0,x,6]/7;
  f=Expand[f0/.{x→x-delta}];
  Clear[a1,a2,a3,a4,a5,a6,a7];
  $f35 = F35 /. AssociationThread[{a1, a2, a3, a4, a5, a6, a7} → Reverse@CoefficientList[f, x,
  factors=FactorList[$f35];
  numbers= Table[Length@Position[Exponent[factors[[All, 1]], x], 7k],{k,1,5}];
  Switch[numbers,{0,0,0,0,1},"Gal=S7/A7", {1,0,0,1,0},"Gal=F168",{0,1,1,0,0},"Gal=F42", {2,0,1,0,
```

### ■ 例1 $x^7-2$

In[240]:=

```
galoisGroup[x7-2]
$f35
Factor[%]
```

Out[240]=

Gal=F<sub>42</sub>

Out[241]=

$4096 - 116\,944 x^7 - 290\,000 x^{14} + 15\,312 x^{21} - 604 x^{28} + x^{35}$

Out[242]=

$(512 - 26 x^7 + x^{14}) (8 - 228 x^7 - 578 x^{14} + x^{21})$

### ■ 例2 $x^7 - 7x^5 + 7x^4 + 7x^3 - 14x^2 + 9$

In[261]:=

```
galoisGroup[x7-7x5+7x4+7x3-14x2+9]
Factor[$f35]
```

Out[261]=

Gal=D<sub>7</sub>

Out[262]=

$(-1 + 7x + 7x^2 + 7x^3 + x^7) (741 - 392x - 231x^2 + 203x^3 + 21x^4 - 28x^5 + x^7)$   
 $(97 - 56x - 84x^2 + 70x^3 + 7x^4 - 14x^5 + x^7) (225 + 735x - 154x^2 - 2261x^3 -$   
 $721x^4 + 1302x^5 + 2450x^6 - 520x^7 - 1127x^8 + 252x^9 + 301x^{10} - 14x^{11} - 28x^{12} + x^{14})$

### ■ 例3 $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

In[256]:=

```
galoisGroup[x7+x6+x5+x4+x3+x2+x+1]
Factor[x7+x6+x5+x4+x3+x2+x+1]
```

Out[256]=

既約ではありません

Out[257]=

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

fが既約でないときは, f35 は7より小さい次数の整式に因子分解できます.

In[260]:=

**Factor[**\$f35**]**

Out[260]=

$$\frac{1}{378\,818\,692\,265\,664\,781\,682\,717\,625\,943} (4 + 7x)^3 (58 - 42x + 49x^2)^2$$

$$(-82 + 56x + 49x^2) (114 + 56x + 49x^2) (20\,808 + 3360x - 2156x^2 - 4116x^3 + 2401x^4)$$

$$(2482 - 756x + 2646x^2 - 4116x^3 + 2401x^4)^2 (5128 - 13\,104x + 17\,052x^2 - 4116x^3 + 2401x^4)$$

$$(1138 - 2324x + 9506x^2 + 5488x^3 + 2401x^4) (12\,114 + 16\,884x + 9506x^2 + 5488x^3 + 2401x^4)$$

## S2 F1, F2,...,F6 の定義と $\sigma, \tau$ による軌道

fの異なる3つの解 $x_i, x_j, x_k$ の和 $(x_i + x_j + x_k)$  ( $0 \leq i < j < k \leq 6$ )の集合をPとおくと、Pの35個の要素は $\langle \sigma \rangle$ による5つの軌道に分解できます。

```
In[*]:= vars = {x0, x1, x2, x3, x4, x5, x6};
orbitByσ[number_, start_List] := "0" <> ToString[number] <> ":" <>
  ToString[Table[Total[vars[[Sort[Mod[start + k, 7]] + 1]]], {k, 0, 6}]]
Column[{orbitByσ[1, {0, 1, 3}], orbitByσ[2, {0, 2, 3}],
  orbitByσ[3, {6, 0, 1}], orbitByσ[4, {5, 0, 2}], orbitByσ[5, {4, 0, 3}]]]
```

```
Out[*]:=
01: {x0 + x1 + x3, x1 + x2 + x4, x2 + x3 +
  x5, x3 + x4 + x6, x0 + x4 + x5, x1 + x5 + x6, x0 + x2 + x6}
02: {x0 + x2 + x3, x1 + x3 + x4, x2 + x4 +
  x5, x3 + x5 + x6, x0 + x4 + x6, x0 + x1 + x5, x1 + x2 + x6}
03: {x0 + x1 + x6, x0 + x1 + x2, x1 + x2 +
  x3, x2 + x3 + x4, x3 + x4 + x5, x4 + x5 + x6, x0 + x5 + x6}
04: {x0 + x2 + x5, x1 + x3 + x6, x0 + x2 +
  x4, x1 + x3 + x5, x2 + x4 + x6, x0 + x3 + x5, x1 + x4 + x6}
05: {x0 + x3 + x4, x1 + x4 + x5, x2 + x5 +
  x6, x0 + x3 + x6, x0 + x1 + x4, x1 + x2 + x5, x2 + x3 + x6}
```

(添え数字だけを見ると、 $O_1$  は  $\{k, k+1, k+3\}$ ,  $O_2$  は  $\{k, k+2, k+3\}$ ,  
 $O_3$  は  $\{k, k+1, k+2\}$ ,  $O_4$  は  $\{k, k+2, k+4\}$ ,  $O_5$  は  $\{k, k+3, k+6\}$  です.)

ここで  $n = 1, 2$  に対し「 $F_n = \prod_{x_i+x_j+x_k \in O_n} (s - (x_i + x_j + x_k))$ 」と定義します。

具体的に書くと次の通りです。

```
In[*]:= F1 =
  (s - (x0 + x1 + x3)) (s - (x1 + x2 + x4)) (s - (x2 + x3 + x5)) (s - (x3 + x4 + x6))
  (s - (x0 + x4 + x5)) (s - (x1 + x5 + x6)) (s - (x0 + x2 + x6));
F2 =
  (s - (x0 + x2 + x3)) (s - (x1 + x3 + x4)) (s - (x2 + x4 + x5)) (s - (x3 + x5 + x6))
  (s - (x0 + x4 + x6)) (s - (x0 + x1 + x5)) (s - (x1 + x2 + x6));
```

$F1, F2$ は $\sigma$ により不変ですが、 $\tau$ により「 $F1 \xrightarrow{\tau} F2, F2 \xrightarrow{\tau} F1$ 」となります。

これは $\tau$ による軌道を見ればわかります。(下参照) 故に $F1$ ,

$F2$ の係数は $F_{21} = \langle \sigma, \tau^2 \rangle$ の固定体に入ります。

```
In[*]:= orbitByτ[number_, start_List] := "0" <> ToString[number] <> ":" <>
ToString[Table[Total[vars[[Sort[Mod[start * 5^k, 7]] + 1]], {k, 0, 6}]]
Column[{orbitByτ[6, {0, 1, 3}], orbitByτ[7, {1, 2, 4}], orbitByτ[8, {2, 3, 5}]]]
```

Out[\*]=

```
06: {x0 + x1 + x3, x0 + x1 + x5, x0 + x4 +
     x5, x0 + x4 + x6, x0 + x2 + x6, x0 + x2 + x3, x0 + x1 + x3}
07: {x1 + x2 + x4, x3 + x5 + x6, x1 + x2 +
     x4, x3 + x5 + x6, x1 + x2 + x4, x3 + x5 + x6, x1 + x2 + x4}
08: {x2 + x3 + x5, x1 + x3 + x4, x1 + x5 +
     x6, x2 + x4 + x5, x3 + x4 + x6, x1 + x2 + x6, x2 + x3 + x5}
```

03の要素は $\tau$ により 03, 04, 05 の間を動きます.04,05の要素も同様です.

## §3 $f_1, f_2$ の見つけ方

以下「 $a_1=0$ 」と仮定します。したがって「 $x_0+x_1+x_2+x_3+x_4+x_5+x_6=0$ 」です。また  $F_{35}, F_1, F_2$  の様に一般的な関数の時は大文字で、具体的な関数  $f$  に適用したときは  $f_{35}, f_1, f_2$  の様に小文字で表すものとします。（ただしはっきりと区別されてないときもあります）

### §3-1 $\text{Gal} = F_{42}, F_{21}, D_7$ のとき

これらの場合は簡単です。（「同じ軌道の上にある  $m$  個の解は、既約な  $m$  次方程式を作るか一次式  $m$  個に分解できる」ので直感的には明らかです。）

■  $\text{Gal} = F_{42}$  のとき

$f_{35}$  は  $(14 + 21)$  次の式に分かれますが、 $14$  次の式は、  
その判別式を  $D$  とすると  $Q(\sqrt{D})$  上で  $(7 + 7)$  次の2式に因数分解されます。これらが  $f_1$  と  $f_2$  です

■  $\text{Gal} = F_{21}$  のとき

$f_{35}$  は  $(7 + 7 + 21)$  次の式に分かれますが、この2つの7次の式が  $f_1$  と  $f_2$  です

■  $\text{Gal} = D_7$  のとき

$f_{35}$  は  $(7 + 7 + 7 + 14)$  次の式に分かれますが、 $14$  次の式は、  
その判別式を  $D$  とすると  $Q(\sqrt{D})$  上で  $(7 + 7)$  次の2式に因数分解されます。これらが  $f_1$  と  $f_2$  です

### §3-2 $\text{Gal} = C_7$ のとき

この場合はかなり面倒です。

#### §3-2-1 $O_1 \sim O_5$ と共通項 $x_k$

$\text{Gal} = C_7$  のとき、 $f_{35}$  は  $(7 + 7 + 7 + 7 + 7)$  次の式に分かれます。このうち  $f_1$  と  $f_2$  を見つけるには、 $P$  の2つの要素がある項  $x_k$  ( $0 \leq k \leq 6$ ) を共有するか否かを考える必要があります。 $O_i$  の軌道より

(ア)  $O_1$  と  $O_j$  ( $j = 2, 3, 4, 5$ ) の場合

$O_1$  の各々の要素  $s$  について、 $s$  と共通の  $x_k$  がない  $O_j$  の要素  $t$  がただ一つ存在します

(例えば  $j = 2$  のとき、 $s = x_0 + x_1 + x_3$  とすると  $t = x_2 + x_4 + x_5$ )

(イ)  $O_2$  と  $O_j$  ( $j = 1, 3, 4, 5$ ) の場合

「1」と同様です。 $O_2$  の各々の要素  $s$  について、 $s$  と共通の  $x_k$  がない  $O_j$  の要素  $t$  がただ一つ存在します

(ウ)  $O_i$  と  $O_j$  ( $3 \leq i, j \leq 5, i \neq j$ ) の場合

$O_i$  の各々の要素  $s$  について、 $O_j$  の任意の要素は  $s$  と共通の  $x_k$  を持ちます。

(例えば  $O_3, s = x_0 + x_1 + x_6$  のとき、

$O_4$  の任意の要素を  $t$  とすると  $s$  と  $t$  は必ず共通の  $x_k$  が有ります。)

$O_i, O_j$  ( $1 \leq i, j \leq 5, i \neq j$ ) の任意の要素をそれぞれ  $s, t$  とすると、 $s$  と  $t$  に共通項  $x_k$  が無いとき、

ある  $m$  ( $0 \leq m \leq 6$ ) について「 $s + t + x_m = x_0 + x_1 + \cdots + x_6 = 0$ 」が成り立ちます.

このとき「 $f(-s-t) = f(x_m) = 0$ 」です.

逆に「 $s, t$ に共通項がありかつ  $f(-s-t) = 0$ 」のときは  $-s-t = x_m$  より

「 $(\#) c_0 x_0 + c_1 x_1 + c_2 x_2 + \cdots + c_6 x_6 = 0$  ( $c_k \geq 0$ , ある  $i, j$  について  $c_i \neq c_j$ )」です.

ところが  $Gal = C_7$  ですから  $(\#)$  の両辺を  $\sigma$  で繰り返し移すと,

「 $c_6 x_0 + c_0 x_1 + c_1 x_2 + \cdots + c_5 x_6 = 0$ ,  $\cdots$ ,  $c_1 x_0 + c_2 x_1 + c_3 x_2 + \cdots + c_0 x_6 = 0$ 」

が成り立ちます. ゆえに巡回行列の性質から「 $c_0 = c_1 = \cdots = c_6$ 」となり,

矛盾します. (詳しくは原論文参照) 即ち

( $\#2$ )  $0_i, 0_j$  ( $1 \leq i, j \leq 5, i \neq j$ ) の任意の要素をそれぞれ  $s$ ,  
 $t$  とすると「 $s$ と $t$ に共通項 $x_k$ が無い  $\Leftrightarrow f(-s-t) = 0$ 」です

### §3-2-2 $Gal = C_7$ のときの $f_1, f_2$ の見つけ方

$f_{35}$  を因数分解した式を, 適当に  $h_1(x), h_2(x), \dots$ ,

$h_5(x)$  と名付けます.  $h_1(s)$  と  $f(-s-t)$  の終結式を  $R(t)$  とすると, 上から,

( $\#3$ )  $h_1(x)$  の解と  $h_2(x)$  の解が  $0_1$  と  $0_j$  ( $j = 2, 3, 4, 5$ ) または  $0_2$  と  $0_j$   
 ( $j = 1, 3, 4, 5$ )  $\Leftrightarrow$  「 $h_1(s) = 0, h_2(t) = 0, f(-s-t) = 0$ 」を満たすある  $s$ ,  
 $t$  が存在する」 $\Leftrightarrow$  「 $R(t)$  が  $h_2(t)$  で割り切れる」

となります.

( $\because$  「 $h_1(s) = 0$ 」と「 $f(-s-t) = 0$ 」が共通解を持つ  $t$  の条件が「 $R(t) = 0$ 」なので,  
 「 $h_2(t) \mid R(t)$ 」のとき, 「 $h_1(s) = h_2(t) = f(-s-t) = 0$ 」が成り立ちます.)

したがって以下の様にして  $f_1, f_2$  を見つけることができます.

$R(t)$  を  $h_1(s)$  と  $f(-s-t)$  の  $s$  に関する終結式,

$H = \{h_2(t), h_3(t), h_4(t)\}$  のうち  $R(t)$  を割り切る整式の個数を  $N$  とします.

このとき  $N = 0$  はあり得ません.

- $N = 2$  のとき,  $H$  のうち  $R(t)$  を割り切る2個の整式が  $f_1$  と  $f_2$  です.
- $N = 1$  のとき,  $H$  のうち  $R(t)$  を割り切る1個の整式と  $h_5$  が  $f_1$  と  $f_2$  です.
- $N = 3$  のとき, これだけでは決まりません. 次に  $R_2(t)$  を  $h_2(s)$  の  $s$  に関する終結式として,  
 $H_2 = \{h_3(t), h_4(t), h_5(t)\}$  のうち  $R_2(t)$  を割り切る整式の個数を  $M$  とします.  
 このとき  $M = 1$  なら  $H_2$  のうち  $R_2(t)$  を割り切る1個の整式と  $h_1$  が  $f_1$  と  $f_2$  です.  
 $M = 3$  なら  $h_1$  と  $h_2$  が  $f_1$  と  $f_2$  です.  $M = 0, 2$  はあり得ません.

### §3-2-3 $f_1, f_2$ の係数の体

以上の求め方より  $f_1, f_2$  の係数は  $Q(\sqrt{D})$  ( $D$ は $f$ の判別式) に入ることが分かります.

## §4. $f_1, f_2$ を見つけるプログラム

### §4-1 $\text{Gal} = F_{42}, F_{21}, D_7$ のとき

私は何週間もSageMathを使って 可解で既約な7次方程式を探してきましたが、  
 今までのところ  $\text{Gal} = F_{42}, D_7$  の場合しか見つかりません。  
 $\text{Gal} = F_{21}, C_7$  のケースもあるはずなのですが、まだ見つかりません。

**【例1】**  $\text{Gal} = F_{42}$  の方程式「 $x^7 - 2x^5 + x^4 + 4x^3 - x^2 - 4x + 3 = 0$ 」  
 に対して  $f_{35}$  を求めて因数分解してみます。

```
In[*]:= f35 = F35 /. AssociationThread[{a1, a2, a3, a4, a5, a6, a7} -> {0, -2, 1, 4, -1, -4, 3}]
Out[*]:=
15 111 - 276 132 x + 1 426 637 x^2 - 3 680 789 x^3 + 4 781 023 x^4 - 863 982 x^5 - 6 771 888 x^6 +
9 142 466 x^7 - 937 547 x^8 - 8 716 581 x^9 + 7 475 377 x^10 + 2 428 894 x^11 - 7 106 606 x^12 +
2 272 884 x^13 + 3 476 289 x^14 - 2 909 525 x^15 - 415 490 x^16 + 1 819 025 x^17 - 422 522 x^18 -
537 798 x^19 + 420 339 x^20 + 120 094 x^21 - 137 300 x^22 + 13 676 x^23 + 44 668 x^24 -
8463 x^25 - 9548 x^26 + 2175 x^27 + 978 x^28 - 643 x^29 - 26 x^30 + 148 x^31 + 2 x^32 - 20 x^33 + x^35

In[*]:= factored = Factor[f35]
Out[*]:=
(207 - 102 x - 67 x^2 + 887 x^3 + 473 x^4 -
472 x^5 + 15 x^6 + 415 x^7 + 65 x^8 - 58 x^9 + 19 x^10 + 6 x^11 - 8 x^12 + x^14)
(73 - 1298 x + 6276 x^2 - 15 422 x^3 + 22 924 x^4 - 21 630 x^5 + 12 825 x^6 - 5247 x^7 + 4299 x^8 - 5985 x^9 +
5329 x^10 - 2439 x^11 + 430 x^12 + 113 x^13 + 321 x^14 - 192 x^15 + 72 x^16 + 33 x^17 - 4 x^18 - 12 x^19 + x^21)
```

このうち 14 次の方程式が  $f_1 * f_2$  ( $f_{12}$ と表記) です。

```
In[*]:= f12 = (List @@ factored)[1]
Out[*]:=
207 - 102 x - 67 x^2 + 887 x^3 + 473 x^4 - 472 x^5 + 15 x^6 + 415 x^7 + 65 x^8 - 58 x^9 + 19 x^10 + 6 x^11 - 8 x^12 + x^14
```

$f_{12}$ の判別式の平方根をdとします。

```
In[*]:= d = Discriminant[f12, x] // Sqrt
Out[*]:=
101 337 771 315 350 603 978 217 i sqrt(91)
```

$Q(d)$  上で  $f_{12}$  を因数分解します。

```
In[*]:= factored2 = Factor[f12, Extension -> d]
Out[*]:=
1
4 (3 i + 3 sqrt(91) + (23 i - sqrt(91)) x + (34 i - 2 sqrt(91)) x^2 + (-3 i + 3 sqrt(91)) x^3 +
(-6 i + 2 sqrt(91)) x^4 + 8 i x^5 - 2 i x^7) (-3 i + 3 sqrt(91) + (-23 i - sqrt(91)) x +
(-34 i - 2 sqrt(91)) x^2 + (3 i + 3 sqrt(91)) x^3 + (6 i + 2 sqrt(91)) x^4 - 8 i x^5 + 2 i x^7)
```

故に  $f_1, f_2$  は以下の様にとれます。(逆に選ぶことももちろん可能)



```
In[ ]:= f1 = (List @@ factored2) [[2]] / (-2 I) // Expand
```

```
Out[ ]:=
```

$$-\frac{3}{2} + \frac{3 \sqrt{91}}{2} - \frac{23x}{2} - \frac{1}{2} \sqrt{91} x - 17x^2 - \sqrt{91} x^2 + \frac{3x^3}{2} + \frac{3}{2} \sqrt{91} x^3 + 3x^4 + \sqrt{91} x^4 - 4x^5 + x^7$$

```
In[ ]:= f2 = (List @@ factored2) [[3]] / (2 I) // Expand
```

```
Out[ ]:=
```

$$-\frac{3}{2} - \frac{3 \sqrt{91}}{2} - \frac{23x}{2} + \frac{1}{2} \sqrt{91} x - 17x^2 + \sqrt{91} x^2 + \frac{3x^3}{2} - \frac{3}{2} \sqrt{91} x^3 + 3x^4 - \sqrt{91} x^4 - 4x^5 + x^7$$

【例2】 $\text{Gal} = F_{14} = D_7$  の方程式「 $x^7 + 4x^4 + x^3 - 2x^2 + 2x + 3 = 0$ 」  
に対して  $f_{35}$  を求めて因数分解してみます。

```
In[ ]:= f35 = F35 /. AssociationThread[{a1, a2, a3, a4, a5, a6, a7} -> {0, 0, 4, 1, -2, 2, 3}]
```

```
Out[ ]:=
```

$$31104 - 456192x + 2460672x^2 - 6314400x^3 + 8701608x^4 - 5329568x^5 - 1558016x^6 + 4343495x^7 + 1410916x^8 - 7779816x^9 + 4672350x^{10} + 3918452x^{11} - 3562668x^{12} - 1014192x^{13} + 1955754x^{14} + 493776x^{15} - 269874x^{16} + 571536x^{17} + 812340x^{18} + 333945x^{19} + 195750x^{20} + 110184x^{21} + 50280x^{22} - 14064x^{23} + 78x^{24} - 1692x^{25} + 684x^{26} - 258x^{27} + 834x^{28} + 32x^{29} + 20x^{30} - 8x^{31} + 8x^{32} + x^{35}$$

```
In[ ]:= factored = Factor[f35]
```

```
Out[ ]:=
```

$$(27 - 54x + 18x^2 + 29x^3 + 2x^4 - 10x^5 + x^7) (-1 + 8x - 16x^2 + 15x^3 - 6x^4 + 2x^5 + x^7) (-9 + 42x + 2x^2 + 25x^3 + 2x^4 + 8x^5 + x^7) (128 + 160x^3 + 56x^4 + 352x^6 + 469x^7 + 176x^8 + 7x^{10} + 10x^{11} + x^{14})$$

このうち 14 次の方程式が  $f_1 \cdot f_2$  ( $f_{12}$ と表記) のはずです。

```
In[ ]:= f12 = (List @@ factored) [[4]]
```

```
Out[ ]:=
```

$$128 + 160x^3 + 56x^4 + 352x^6 + 469x^7 + 176x^8 + 7x^{10} + 10x^{11} + x^{14}$$

$f_{12}$ の判別式の平方根をdとします。

```
In[ ]:= d = Discriminant[f12, x] // Sqrt
```

```
Out[ ]:=
```

$$794690010491513998348910592 \sqrt{151}$$

$\mathbb{Q}(d)$  上で  $f_{12}$  を因数分解します。

```
In[ ]:= factored2 = Factor[f12, Extension -> d]
```

```
Out[ ]:=
```

$$\frac{1}{4} (19 \sqrt{151} + (-7 \sqrt{151} + 3 \sqrt{151}) x^3 + (-10 \sqrt{151} + 2 \sqrt{151}) x^4 - 2 \sqrt{151} x^7) (-19 \sqrt{151} + (7 \sqrt{151} + 3 \sqrt{151}) x^3 + (10 \sqrt{151} + 2 \sqrt{151}) x^4 + 2 \sqrt{151} x^7)$$

故に  $f_1, f_2$  は以下の様にとれます。(逆に選ぶことももちろん可能)

In[\*]:= **f1 = (List @@ factored2) [[2]] / (-2 I) // Expand**

Out[\*]:=

$$-\frac{19}{2} + \frac{i\sqrt{151}}{2} + \frac{7x^3}{2} + \frac{3}{2}i\sqrt{151}x^3 + 5x^4 + i\sqrt{151}x^4 + x^7$$

In[\*]:= **f2 = (List @@ factored2) [[3]] / (2 I) // Expand**

Out[\*]:=

$$-\frac{19}{2} - \frac{i\sqrt{151}}{2} + \frac{7x^3}{2} - \frac{3}{2}i\sqrt{151}x^3 + 5x^4 - i\sqrt{151}x^4 + x^7$$

**【プログラム】**  $\text{Ga1} = F_{14}$ ,  $D_7$  に対しては次のプログラムで  $\{f_1, f_2\}$  が求まります。

```
In[*]:= findF12[f_] := Module[{f35, factors, pos1, pos2, f12, d, f12factors},
  f35 = F35 /. AssociationThread[{a1, a2, a3, a4, a5, a6, a7} → Reverse@CoefficientList[f, x],
  factors = FactorList[f35];
  pos1 = Position[Exponent[factors[[All, 1]], x], 14][[1, 1]];
  f12 = factors[[pos1]][[1]];
  d = Sqrt@Discriminant[f12, x];
  f12factors = FactorList[f12, Extension → d];
  pos2 = Flatten@Position[Exponent[f12factors[[All, 1]], x], 7];
  (Expand[#[Coefficient[#, x, 7]] &] /@f12factors
  [[pos2]][[All, 1]]
  ]
```

In[\*]:= **findF12** $[x^7 - 2x^5 + x^4 + 4x^3 - x^2 - 4x + 3]$

**findF12** $[x^7 + 4x^4 + x^3 - 2x^2 + 2x + 3]$

Out[\*]:=

$$\left\{ -\frac{3}{2} - \frac{3i\sqrt{91}}{2} - \frac{23x}{2} + \frac{1}{2}i\sqrt{91}x - 17x^2 + i\sqrt{91}x^2 + \frac{3x^3}{2} - \frac{3}{2}i\sqrt{91}x^3 + 3x^4 - i\sqrt{91}x^4 - 4x^5 + x^7, -\frac{3}{2} + \frac{3i\sqrt{91}}{2} - \frac{23x}{2} - \frac{1}{2}i\sqrt{91}x - 17x^2 - i\sqrt{91}x^2 + \frac{3x^3}{2} + \frac{3}{2}i\sqrt{91}x^3 + 3x^4 + i\sqrt{91}x^4 - 4x^5 + x^7 \right\}$$

Out[\*]:=

$$\left\{ -\frac{19}{2} - \frac{i\sqrt{151}}{2} + \frac{7x^3}{2} - \frac{3}{2}i\sqrt{151}x^3 + 5x^4 - i\sqrt{151}x^4 + x^7, -\frac{19}{2} + \frac{i\sqrt{151}}{2} + \frac{7x^3}{2} + \frac{3}{2}i\sqrt{151}x^3 + 5x^4 + i\sqrt{151}x^4 + x^7 \right\}$$

## §4-2 Gal = C<sub>7</sub> のとき

Mathematicaでは、終結式は `Resultant` になります。下の「例2」の使い方をします。

`In[*]:= Resultant[poly1, poly2, var]`  
 多項式  $poly_1$  と  $poly_2$  の変数  $var$  に関する終結式を計算する。

`In[*]:=` 主係数を1とする2つの多項式  $p$  と  $q$  の終結式は、  
 すべての多項式の解の差  $p_i - q_j$  の積である。終結式は必ず数または多項式になる。

【例1】`Resultant[(x - a) (x - b), (x - d) (x - c), x] → (b - c) (-a + c) (b - d) (-a + d)`  
`Resultant[(x - a) (x - b), (x - a) (x - c), x] → 0`

【例2】2つの多項式が共通根を持つ条件を求める：

`Resultant[x^2 - 2 a x^2 + a^2 x - 1, x^2 - 2 a x + 3, x] →`  
 $16 - 48 a + 32 a^2 + 12 a^3 - 9 a^4$   
`a /. Solve[% == 0, a] →  $\left\{-2, \frac{2}{3}, \frac{2}{3}, 2\right\}$`

実例をお見せしたいのですが、

未だに  $\text{Gal} = C_7$  の方程式は見つかっていないのでお見せできません。（^^;）しかし  $f_{35} = h_1 h_2 h_3 h_4 h_5$ （ $h_i$  は  $\mathbb{Q}$  上既約な7次方程式で関数形式）と因数分解できたとなると、  
 §3-2 より、 $f_1, f_2$  は次の様にして求まるはずで。

```
R1 = Resultant[f[-s - t], h1[s], s];
pos = Position[PolynomialRemainder[R1, #, t] & /@ {h2[t], h3[t], h4[t]}, 0] // Flatten;
Which[Length[pos] == 2, pos + 1, Length[pos] == 1, {pos[[1]] + 1, 5}, Length[pos] == 3, R2 =
Resultant[f[-s - t], h2[s], s]; Flatten@Position[PolynomialRemainder[R2, #, t] & /@ {h3[t],
h4[t], h5[t]}, 0];
If[Length[pos2] == 1, {1, pos2[[1]] + 2}, {1, 2}]]
```

## §5. F3

### §5-1 F3の定義と求め方

解が「 $(x_0 + x_1 + x_3) - (x_2 + x_4 + x_5)$ 」の $\sigma$ による軌道となっている7次方程式を F3 と定義します。すなわち

$$\begin{aligned} In[*] := F3 = & (x - (x_0 + x_1 + x_3) + (x_2 + x_4 + x_5)) \\ & (x - (x_1 + x_2 + x_4) + (x_3 + x_5 + x_6)) (x - (x_2 + x_3 + x_5) + (x_0 + x_4 + x_6)) \\ & (x - (x_3 + x_4 + x_6) + (x_1 + x_5 + x_0)) (x - (x_0 + x_4 + x_5) + (x_1 + x_2 + x_6)) \\ & (x - (x_1 + x_5 + x_6) + (x_0 + x_2 + x_3)) (x - (x_0 + x_2 + x_6) + (x_1 + x_3 + x_4)); \end{aligned}$$

F3の解は、 $x_k$  という共通項を持たない F1の解とF2の解の差となっています。なお、F3は  $r_3, r_5, r_6$  を  $r_1$  の式で表すときにしか使わないので、数値計算を使って厳密解を求める際には不要です。

定義より  $\tau$  により  $F3 \xrightarrow{\tau} -F3$  だから、F3は  $F_{21} = < \sigma$ ,  $\tau^2 >$  によって動きません。即ち F3の係数は  $F_{21}$  の固定体に属します。

F3を求めるには  $Gal = C_7$  のときに  $f_1$ ,  $f_2$  を求めたのと同様のやり方が使えます。 $f_1, f_2$ の解を  $s_1, s_2$  とすると、「 $s_1$  と  $s_2$  が 共通の項  $x_k$  を持たない  $\Leftrightarrow f(-s_1 - s_2) = 0$ 」なので  $f_3$ の解を  $t$  とすると

$$(\#4) \text{ ある } s_1, s_2 \text{ に対して } f_1(s_1) = 0 \wedge f_2(s_2) = 0 \wedge f(-s_1 - s_2) = 0 \wedge t = s_1 - s_2$$

これから  $s_1, s_2$  を消去して  $t$  の条件を求めると、 $t$  の7次方程式が得られるはずで、その変数を  $x$  に変えた式が  $f_3$  です。これも 終結式を使って求められます。

「 $-s_1 - s_2 = x, s_1 - s_2 = t$ 」とおくと「 $s_1 = (t - x) / 2, s_2 = (-t - x) / 2$ 」だから、  
 $R_1(t)$  を「 $f(x)$  と  $f_1((t - x) / 2)$  の  $x$  についての終結式」、  
 $R_2(t)$  を「 $f(x)$  と  $f_1((t - x) / 2)$  の  $x$  についての終結式」とすると、  
 $t$  の条件は以下の  $(\#4)'$ ,  $(\#4)''$  と同値です。

$$\begin{aligned} (\#4)' \text{ ある } x \text{ に対して} \\ f_1((t - x) / 2) = 0 \wedge f_2((-t - x) / 2) = 0 \wedge f(x) = 0 \text{ が成り立つ} \end{aligned}$$

$$(\#4)'' R_1(t) \text{ と } R_2(t) \text{ の } GCD = 0 \text{ (GCDは最大公約因数)}$$

なぜなら「 $R_1(t)$  と  $R_2(t)$  の  $GCD = 0$ 」のとき「 $R_1(t) = 0$  かつ  $R_2(t) = 0$ 」で、  
 このとき「 $f = 0$  と  $f_1((t - x) / 2) = 0$  が共通解を持ち、  
 かつ、 $f = 0$  と  $f_2((-t - x) / 2) = 0$  が共通解を持つ」ので  
 「 $f = 0, f_1((t - x) / 2) = 0, f_2((-t - x) / 2) = 0$  が共通解を持つ」からです。

## §5-2 【例】 $\text{Ga1} = \text{F}_{42}$ の方程式「 $x^7 - 2x^5 + x^4 + 4x^3 - x^2 - 4x + 3 = 0$ 」

`In[*]:= f[x_] = x7 - 2 x5 + x4 + 4 x3 - x2 - 4 x + 3;`

§4-1 より, f1, f2は次の様になります .

`In[*]:= Clear[f1, f2]`

$$f1[x_] = -\frac{3}{2} + \frac{3\sqrt{91}}{2} - \frac{23x}{2} - \frac{1}{2}\sqrt{91}x -$$

$$17x^2 - \sqrt{91}x^2 + \frac{3x^3}{2} + \frac{3}{2}\sqrt{91}x^3 + 3x^4 + \sqrt{91}x^4 - 4x^5 + x^7;$$

$$f2[x_] = -\frac{3}{2} - \frac{3\sqrt{91}}{2} - \frac{23x}{2} + \frac{1}{2}\sqrt{91}x -$$

$$17x^2 + \sqrt{91}x^2 + \frac{3x^3}{2} - \frac{3}{2}\sqrt{91}x^3 + 3x^4 - \sqrt{91}x^4 - 4x^5 + x^7;$$

R1, R2は次の様になります .

```
In[*]:= R1 = Resultant[f[x], f1[(t - x) / 2], x]
R2 = Resultant[f[x], f2[(-t - x) / 2], x]
```

```
Out[*]=
```

$$\frac{1}{562\,949\,953\,421\,312} \left( 27\,449\,661\,829\,098\,843\,571\,419 + 16\,596\,156\,655\,212\,155\,115\,120 \sqrt{91} + 87\,455\,883\,607\,650\,744\,465\,396 t + 80\,795\,356\,198\,919\,187\,918\,608 \sqrt{91} t + 254\,440\,636\,221\,417\,602\,094\,801 t^2 + 111\,374\,554\,675\,240\,628\,806\,096 \sqrt{91} t^2 + 497\,642\,719\,038\,916\,324\,887\,780 t^3 + 28\,322\,536\,318\,936\,299\,986\,064 \sqrt{91} t^3 + 444\,121\,743\,273\,133\,563\,484\,582 t^4 - 57\,712\,552\,054\,367\,160\,544\,408 \sqrt{91} t^4 - 37\,737\,110\,616\,370\,956\,218\,050 t^5 - 36\,648\,007\,002\,143\,913\,276\,368 \sqrt{91} t^5 - 354\,098\,844\,597\,833\,517\,658\,473 t^6 + 22\,646\,452\,435\,824\,087\,908\,232 \sqrt{91} t^6 - 175\,992\,488\,585\,689\,430\,270\,737 t^7 + 28\,950\,875\,726\,745\,618\,678\,704 \sqrt{91} t^7 + 55\,295\,748\,812\,619\,805\,693\,249 t^8 + 3\,719\,632\,463\,657\,520\,059\,248 \sqrt{91} t^8 + 52\,818\,963\,536\,984\,361\,083\,412 t^9 - 6\,398\,434\,402\,608\,597\,217\,056 \sqrt{91} t^9 - 14\,766\,850\,702\,217\,011\,115\,878 t^{10} - 3\,229\,529\,090\,543\,785\,771\,544 \sqrt{91} t^{10} - 18\,785\,808\,297\,825\,593\,327\,957 t^{11} - 504\,502\,075\,773\,602\,793\,992 \sqrt{91} t^{11} + 2\,992\,178\,495\,819\,422\,969\,743 t^{12} + 368\,888\,216\,111\,490\,638\,208 \sqrt{91} t^{12} + 8\,231\,499\,966\,678\,837\,609\,306 t^{13} + 350\,949\,643\,922\,966\,137\,280 \sqrt{91} t^{13} + 1\,669\,624\,603\,972\,880\,057\,050 t^{14} - 68\,502\,886\,757\,883\,627\,048 \sqrt{91} t^{14} - 1\,588\,947\,898\,765\,901\,246\,862 t^{15} - 154\,891\,172\,977\,425\,010\,920 \sqrt{91} t^{15} - 483\,113\,377\,319\,593\,873\,744 t^{16} - 25\,484\,421\,474\,975\,702\,384 \sqrt{91} t^{16} + 255\,787\,499\,836\,712\,019\,996 t^{17} + 12\,430\,957\,473\,742\,358\,672 \sqrt{91} t^{17} + 43\,843\,260\,282\,099\,847\,065 t^{18} - 817\,632\,185\,811\,594\,624 \sqrt{91} t^{18} - 54\,963\,444\,923\,764\,635\,431 t^{19} - 2\,289\,400\,316\,158\,836\,040 \sqrt{91} t^{19} - 6\,292\,470\,736\,330\,491\,611 t^{20} - 217\,811\,347\,673\,446\,992 \sqrt{91} t^{20} + 4\,246\,869\,260\,422\,243\,809 t^{21} + 104\,741\,254\,857\,516\,576 \sqrt{91} t^{21} - 1\,606\,857\,960\,372\,773\,082 t^{22} + 120\,170\,922\,276\,676\,648 \sqrt{91} t^{22} - 774\,303\,375\,653\,278\,246 t^{23} + 35\,867\,910\,194\,829\,128 \sqrt{91} t^{23} + 236\,775\,802\,379\,631\,567 t^{24} - 10\,930\,907\,732\,726\,280 \sqrt{91} t^{24} + 84\,730\,051\,592\,978\,298 t^{25} + 1\,503\,429\,893\,444\,752 \sqrt{91} t^{25} - 15\,029\,518\,416\,409\,926 t^{26} + 3\,741\,221\,052\,187\,944 \sqrt{91} t^{26} - 4\,568\,715\,222\,988\,215 t^{27} - 239\,023\,998\,056\,520 \sqrt{91} t^{27} + 1\,649\,210\,889\,776\,268 t^{28} - 441\,932\,341\,445\,768 \sqrt{91} t^{28} + 776\,749\,000\,174\,901 t^{29} + 29\,519\,029\,677\,296 \sqrt{91} t^{29} - 30\,190\,801\,804\,356 t^{30} + 30\,628\,808\,442\,168 \sqrt{91} t^{30} - 78\,462\,286\,138\,317 t^{31} - 4\,514\,417\,653\,200 \sqrt{91} t^{31} - 1\,152\,872\,597\,249 t^{32} - 2\,280\,171\,676\,328 \sqrt{91} t^{32} + 5\,816\,849\,538\,096 t^{33} + 167\,719\,285\,824 \sqrt{91} t^{33} - 183\,647\,597\,908 t^{34} + 120\,971\,799\,816 \sqrt{91} t^{34} - 388\,817\,755\,409 t^{35} - 1\,144\,036\,824 \sqrt{91} t^{35} + 10\,415\,144\,388 t^{36} - 5\,966\,202\,888 \sqrt{91} t^{36} + 16\,178\,508\,683 t^{37} - 92\,037\,696 \sqrt{91} t^{37} - 478\,959\,973 t^{38} + 330\,768\,736 \sqrt{91} t^{38} - 485\,940\,429 t^{39} + 10\,910\,064 \sqrt{91} t^{39} + 12\,677\,139 t^{40} - 12\,492\,496 \sqrt{91} t^{40} + 14\,419\,700 t^{41} - 129\,360 \sqrt{91} t^{41} + 511\,197 t^{42} + 324\,408 \sqrt{91} t^{42} - 344\,503 t^{43} - 9528 \sqrt{91} t^{43} - 22\,395 t^{44} - 6192 \sqrt{91} t^{44} + 7032 t^{45} + 168 \sqrt{91} t^{45} + 175 t^{46} + 56 \sqrt{91} t^{46} - 126 t^{47} + t^{49} )$$

```
Out[*]=
```

$$\frac{1}{562\,949\,953\,421\,312} \left( 27\,449\,661\,829\,098\,843\,571\,419 - 16\,596\,156\,655\,212\,155\,115\,120 \sqrt{91} - 87\,455\,883\,607\,650\,744\,465\,396 t + 80\,795\,356\,198\,919\,187\,918\,608 \sqrt{91} t + 254\,440\,636\,221\,417\,602\,094\,801 t^2 - 111\,374\,554\,675\,240\,628\,806\,096 \sqrt{91} t^2 - 497\,642\,719\,038\,916\,324\,887\,780 t^3 + 28\,322\,536\,318\,936\,299\,986\,064 \sqrt{91} t^3 + 444\,121\,743\,273\,133\,563\,484\,582 t^4 + 57\,712\,552\,054\,367\,160\,544\,408 \sqrt{91} t^4 + 37\,737\,110\,616\,370\,956\,218\,050 t^5 - 36\,648\,007\,002\,143\,913\,276\,368 \sqrt{91} t^5 - 354\,098\,844\,597\,833\,517\,658\,473 t^6 - 22\,646\,452\,435\,824\,087\,908\,232 \sqrt{91} t^6 + 175\,992\,488\,585\,689\,430\,270\,737 t^7 + 28\,950\,875\,726\,745\,618\,678\,704 \sqrt{91} t^7 + 55\,295\,748\,812\,619\,805\,693\,249 t^8 - 3\,719\,632\,463\,657\,520\,059\,248 \sqrt{91} t^8 - 52\,818\,963\,536\,984\,361\,083\,412 t^9 - 6\,398\,434\,402\,608\,597\,217\,056 \sqrt{91} t^9 - 14\,766\,850\,702\,217\,011\,115\,878 t^{10} + 3\,229\,529\,090\,543\,785\,771\,544 \sqrt{91} t^{10} + 18\,785\,808\,297\,825\,593\,327\,957 t^{11} - 504\,502\,075\,773\,602\,793\,992 \sqrt{91} t^{11} + 2\,992\,178\,495\,819\,422\,969\,743 t^{12} - 368\,888\,216\,111\,490\,638\,208 \sqrt{91} t^{12} - 8\,231\,499\,966\,678\,837\,609\,306 t^{13} + 350\,949\,643\,922\,966\,137\,280 \sqrt{91} t^{13} + 1\,669\,624\,603\,972\,880\,057\,050 t^{14} + 68\,502\,886\,757\,883\,627\,048 \sqrt{91} t^{14} + 1\,588\,947\,898\,765\,901\,246\,862 t^{15} - 154\,891\,172\,977\,425\,010\,920 \sqrt{91} t^{15} - 483\,113\,377\,319\,593\,873\,744 t^{16} + 25\,484\,421\,474\,975\,702\,384 \sqrt{91} t^{16} - 255\,787\,499\,836\,712\,019\,996 t^{17} + 12\,430\,957\,473\,742\,358\,672 \sqrt{91} t^{17} + 43\,843\,260\,282\,099\,847\,065 t^{18} + 817\,632\,185\,811\,594\,624 \sqrt{91} t^{18} + 54\,963\,444\,923\,764\,635\,431 t^{19} - 2\,289\,400\,316\,158\,836\,040 \sqrt{91} t^{19} - 6\,292\,470\,736\,330\,491\,611 t^{20} + 217\,811\,347\,673\,446\,992 \sqrt{91} t^{20} - 4\,246\,869\,260\,422\,243\,809 t^{21} + 104\,741\,254\,857\,516\,576 \sqrt{91} t^{21} - 1\,606\,857\,960\,372\,773\,082 t^{22} - 120\,170\,922\,276\,676\,648 \sqrt{91} t^{22} + 774\,303\,375\,653\,278\,246 t^{23} + 35\,867\,910\,194\,829\,128 \sqrt{91} t^{23} + 236\,775\,802\,379\,631\,567 t^{24} + 10\,930\,907\,732\,726\,280 \sqrt{91} t^{24} - 84\,730\,051\,592\,978\,298 t^{25} + 1\,503\,429\,893\,444\,752 \sqrt{91} t^{25} - 15\,029\,518\,416\,409\,926 t^{26} - 3\,741\,221\,052\,187\,944 \sqrt{91} t^{26} + 4\,568\,715\,222\,988\,215 t^{27} - 239\,023\,998\,056\,520 \sqrt{91} t^{27} + 1\,649\,210\,889\,776\,268 t^{28} + 441\,932\,341\,445\,768 \sqrt{91} t^{28} - 776\,749\,000\,174\,901 t^{29} + 29\,519\,029\,677\,296 \sqrt{91} t^{29} - 30\,190\,801\,804\,356 t^{30} - 30\,628\,808\,442\,168 \sqrt{91} t^{30} + 78\,462\,286\,138\,317 t^{31} - 4\,514\,417\,653\,200 \sqrt{91} t^{31} - 1\,152\,872\,597\,249 t^{32} + 2\,280\,171\,676\,328 \sqrt{91} t^{32} - 5\,816\,849\,538\,096 t^{33} + 167\,719\,285\,824 \sqrt{91} t^{33} - 183\,647\,597\,908 t^{34} - 120\,971\,799\,816 \sqrt{91} t^{34} + 388\,817\,755\,409 t^{35} - 1\,144\,036\,824 \sqrt{91} t^{35} + 10\,415\,144\,388 t^{36} + 5\,966\,202\,888 \sqrt{91} t^{36} - 16\,178\,508\,683 t^{37} - 92\,037\,696 \sqrt{91} t^{37} - 478\,959\,973 t^{38} - 330\,768\,736 \sqrt{91} t^{38} + 485\,940\,429 t^{39} + 10\,910\,064 \sqrt{91} t^{39} + 12\,677\,139 t^{40} + 12\,492\,496 \sqrt{91} t^{40} - 14\,419\,700 t^{41} - 129\,360 \sqrt{91} t^{41} + 511\,197 t^{42} - 324\,408 \sqrt{91} t^{42} + 344\,503 t^{43} - 9528 \sqrt{91} t^{43} - 22\,395 t^{44} + 6192 \sqrt{91} t^{44} - 7032 t^{45} + 168 \sqrt{91} t^{45} + 175 t^{46} - 56 \sqrt{91} t^{46} + 126 t^{47} - t^{49} )$$

R1とR2のGCDを求めます. このとき「Extension->Automatic」を付けます.

```
In[*]:= PolynomialGCD [poly1, poly2, ..., Extension → Automatic]
```

は各  $poly_i$  に現れる代数的数を含むように係数体を拡大する.

```
In[*]:= gcd = PolynomialGCD[R1, R2, Extension → Automatic]
```

```
Out[*]:= 171  $\sqrt{91}$  - 220  $\sqrt{91}$  t - 79  $\sqrt{91}$  t2 + 56  $\sqrt{91}$  t3 + 7  $\sqrt{91}$  t4 + 14  $\sqrt{91}$  t5 -  $\sqrt{91}$  t7
```

故に

```
In[*]:= f3[x_] = (gcd / (-1) // Expand) /. {t → x}
```

```
Out[*]:= 171  $\sqrt{91}$  + 220 x - 79  $\sqrt{91}$  x2 - 56 x3 + 7  $\sqrt{91}$  x4 - 14 x5 + x7
```

### 【別解】グレブナー基底の利用 (原論文には無いです)

(#4) のイデアルのグレブナー基底を,  $s_1$ ,  
 $s_2$  を消去するモードで作ります. 少し時間がかかります. (4.25 秒)

```
In[*]:= GroebnerBasis[{f1[s1], f2[s2], f[-s1 - s2], t - s1 + s2}, {t}, {s1, s2}] // First
```

```
Out[*]:= 171  $\sqrt{91}$  + 220 t - 79  $\sqrt{91}$  t2 - 56 t3 + 7  $\sqrt{91}$  t4 - 14 t5 + t7
```

或いは, (#4)' のイデアルのグレブナー基底を,  $x$  を消去するモードで作ってもできます. やや速いです. (2.59秒)

```
In[*]:= GroebnerBasis[{f1[(t - x) / 2], f2[(-t - x) / 2], f[x]}, t, x] // First
```

```
Out[*]:= 171  $\sqrt{91}$  + 220 t - 79  $\sqrt{91}$  t2 - 56 t3 + 7  $\sqrt{91}$  t4 - 14 t5 + t7
```

計算時間は, GCDを使う方法が一番速く, 1.57秒でした.

## §5 - 3 F3の係数の体

$f_1, f_2$  の係数は  $Q(\sqrt{D})$  ( $D$ は $f$ の判別式) に入るので,  
 終結式の性質 ( $f$ と $g$ の係数の体が $K$ のとき, その終結式の係数の体は  $K$ に含まれる) から,  
 $R1, R2$ の係数は  $Q(\sqrt{D})$  に入り,  
 そのGCDである  $f_3$  の係数も  $Q(\sqrt{D})$  に入ります. 上の例では「 $\sqrt{D} = 1183 \pm \sqrt{91}$ 」なので,  
 確かに  $f_3(x)$  の係数は  $Q(\sqrt{D})$  に入っています.

```
In[*]:= Discriminant[x7 - 2 x5 + x4 + 4 x3 - x2 - 4 x + 3, x] // Sqrt
```

```
Out[*]:= 1183  $\pm \sqrt{91}$ 
```