G1, G2 を求める　with Mathematica14.0

§0. 準備 (F35)

In[185]:=

```
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, ..., 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 ($0 \le i < j < k \le 6$) 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.

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

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

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.

§1. G1, G2 の定義

fの解を $x_0 \sim x_6$, ξ を1の虚数7乗根とするとき,
Lagrange 分解式は次の様になります. (原論文では Fourier transform と呼んでいます.フランスでは Fourier が発見した事にでもなっているのでしょうか?)

In[187]:=

```
r0 = x0 + x1 + x2 + x3 + x4 + x5 + x6;
r1 = x0 + ξ x1 + ξ^2 x2 + ξ^3 x3 + ξ^4 x4 + ξ^5 x5 + ξ^6 x6;
r2 = x0 + ξ^2 x1 + ξ^4 x2 + ξ^6 x3 + ξ x4 + ξ^3 x5 + ξ^5 x6;
r3 = x0 + ξ ^3 x1 + ξ^6 x2 + ξ^2 x3 + ξ^5 x4 + ξ x5 + ξ^4 x6;
r4 = x0 + ξ^4 x1 + ξ x2 + ξ^5 x3 + ξ^2 x4 + ξ^6 x5 + ξ^3 x6;
r5 = x0 + ξ ^5 x1 + ξ^3 x2 + ξ x3 + ξ^6 x4 + ξ^4 x5 + ξ^2 x6;
r6 = x0 + ξ^6 x1 + ξ^5 x2 + ξ^4 x3 + ξ^3 x4 + ξ^2 x5 + ξ x6;
Clear[ξ]
```

$k = 0, 1, 2, .., 6$ に対し「$\sigma : x_k \to x_{k+1}$, $\tau : x_k \to x_{5k}$」と置くと,

「σ: $r_0 \to r_0$, $r_1 \to \xi^6 r_1$, $r_2 \to \xi^5 r_2$, $r_3 \to \xi^4 r_3$, $r_4 \to \xi^3 r_4$, $r_5 \to \xi^2 r_5$, $r_6 \to \xi r_6$」,
「σ^{-1}: $r_0 \to r_0$, $r_1 \to \xi r_1$, $r_2 \to \xi^2 r_2$, $r_3 \to \xi^3 r_3$, $r_4 \to \xi^4 r_4$, $r_5 \to \xi^5 r_5$, $r_6 \to \xi^6 r_6$」,
「$\tau : r_k \to r_{3k}$, $\tau^2 : r_k \to r_{2k}$」(添え数字はMod7)

故に「$u = r_1 + r_2 + r_4$, $v = r_3 + r_5 + r_6$」とおくと $u \overset{\tau}{\to} v$,

$v \xrightarrow{\tau} u$, また　u, v はτ^2 で不変です．さらに

$$G_1 = (x-u)\,(x-\sigma(u))\,\left(x-\sigma^2(u)\right)\cdots\left(x-\sigma^6(u)\right),$$
$$G_2 = (x-v)\,(x-\sigma(v))\,\left(x-\sigma^2(v)\right)\cdots\left(x-\sigma^6(v)\right)$$

と置くと，「$\zeta^7 = 1$, $\sigma^7 = \mathrm{id}$ （単位元）」より，$k = 0, 1, 2, ..$ に対し

$$\tau_2\left(\sigma^{-k}(u)\right) = \tau^2\left(\zeta^k r_1 + \zeta^{2k} r_2 + \zeta^{4k} r_4\right) =$$
$$\zeta^k r_2 + \zeta^{2k} r_4 + \zeta^{4k} r_1 = \left(\zeta^4\right)^k r_1 + \left(\zeta^4\right)^{2k} r_2 + \left(\zeta^4\right)^{4k} r_4 = \sigma^{-4k}(u)$$
$$\tau_2\left(\sigma^{-k}(v)\right) = \tau^2\left(\zeta^{3k} r_3 + \zeta^{5k} r_5 + \zeta^{6k} r_6\right) =$$
$$\zeta^{3k} r_6 + \zeta^{5k} r_3 + \zeta^{6k} r_5 = \left(\zeta^4\right)^{3k} r_3 + \left(\zeta^4\right)^{5k} r_5 + \left(\zeta^4\right)^{6k} r_6 = \sigma^{-4k}(v)$$

故に G_1, G_2 は $F_{21}=<\sigma,\ \tau^2>$ で不変となります． 具体的に書くと

$$\begin{aligned}
G_1 =\ & (x-(r_1+r_2+r_4))\left(x-\left(\xi r_1+\xi^2 r_2+\xi^4 r_4\right)\right)\left(x-\left(\xi^2 r_1+\xi^4 r_2+\xi r_4\right)\right)\left(x-\left(\xi^3 r_1+\xi^6 r_2+\xi^5 r_4\right)\right)\\
& \left(x-\left(\xi^4 r_1+\xi r_2+\xi^2 r_4\right)\right)\left(x-\left(\xi^5 r_1+\xi^3 r_2+\xi^6 r_4\right)\right)\left(x-\left(\xi^6 r_1+\xi^5 r_2+\xi^3 r_4\right)\right)\\
G_2 =\ & (x-(r_3+r_5+r_6))\left(x-\left(\xi^4 r_3+\xi^2 r_5+\xi r_6\right)\right)\left(x-\left(\xi r_3+\xi^4 r_5+\xi^2 r_6\right)\right)\left(x-\left(\xi^5 r_3+\xi^6 r_5+\xi^3 r_6\right)\right)\\
& \left(x-\left(\xi^2 r_3+\xi r_5+\xi^4 r_6\right)\right)\left(x-\left(\xi^6 r_3+\xi^3 r_5+\xi^5 r_6\right)\right)\left(x-\left(\xi^3 r_3+\xi^5 r_5+\xi^6 r_6\right)\right)
\end{aligned}$$

また τ により， F1とF2，G1とG2 は互いに移ります．

§2. g1, g2 を求める

(公式としてのG1, G2を具体化した関数をg1, g2とします.)

§2-1. 補題

次の補題が必要になります

【補題1】 $r_1 + r_2 + r_4 - (r_3 + r_5 + r_6) = \sqrt{-7}\ (x_1 + x_2 + x_4 - (x_3 + x_5 + x_6))$

(注1) 上の関係式をσ で移した式も成り立ちます. 例えば σ^6 で移すと,

$$(\zeta^6\, r_1 + \zeta^5\, r_2 + \zeta^3\, r_4) - (\zeta^3\, r_3 + \zeta^5\, r_5 + \zeta^6\, r_6) = \sqrt{-7}\ (x_0 + x_1 + x_3 - (x_2 + x_4 + x_5))$$

(注2) $\{r_1,\ r_2,\ r_4\}$ と $\{r_3,\ r_5,\ r_6\}$ の2組に分ける時のみ上のような関係が成り立ちます. 例えば $\{r_1,\ r_2,\ r_3\}$ と $\{r_4,\ r_5,\ r_6\}$ の場合は成り立ちません.

【補題2】 $r_1 + r_2 + r_3 + r_4 + r_5 + r_6 = 7\, x_0$

(注) 上の関係式をσ で移した式も成り立ちます.
例えば σ^6 で移すと「$\zeta\, r_1 + \zeta^2\, r_2 + \zeta^3\, r_3 + \zeta^4\, r_4 + \zeta^5\, r_5 + \zeta^6\, r_6 = 7\, x_6$」となります.

【1 の証明】 単純計算で,
$r_1 + r_2 + r_4 - (r_3 + r_5 + r_6) = (\zeta + \zeta^2 + \zeta^4 - \zeta^3 - \zeta^5 - \zeta^6)\ (x_1 + x_2 + x_4 - x_3 - x_5 - x_6)$
ここで「ζ = Cos[2 / 7 Pi] + I Sin[2 / 7 Pi]」
とすると「$\zeta + \zeta^2 + \zeta^4 - \zeta^3 - \zeta^5 - \zeta^6 = \sqrt{-7}$」です (有名事実).
(注2) に関しては1つずつチェックすればOKと思われますが,
実は私も全てはチェックしていません. (^^;)

【2 の証明】「$1 + \zeta + \zeta^2 + \cdots + \zeta^6 = 1$」だから, r_i の定義式の両辺を加えて,
$r_0 + r_1 + r_2 + r_3 + r_4 + r_5 + r_6 = 7\, x_0$. さらに仮定より $a_1 = 0$ なので, $r_0 = 0$.

§2-2. 終結式とGCD(最大公約因子)を使った求め方

（♯1）「$x_1+x_2+x_4$, $x_3+x_5+x_6$, $r_1+r_2+r_4$, $r_3+r_5+r_6$,
を σ^i (iはある0以上の整数) で移した式を各々 s_1, s_2 , t_1, t_2」とすると,
上の補題から以下の式を満たす f の解x が存在します.

$$
(\sharp 2)\quad \begin{cases} s_1+s_2+x=0 & (ア) \\ t_1+t_2=7x & (イ) \\ t_1-t_2=\sqrt{-7}\,(s_1-s_2) & (ウ) \\ f(x)=0 & (エ) \\ f_1(s_1)=0 & (オ) \\ f_2(s_2)=0 & (カ) \end{cases}
$$

「（♯1） → （♯2）」は明らかですが, 逆に（♯1）が成り立てば（♯2）が成り立ちそうです.
(以下は厳密な証明ではありません) というのも,
まず (オ) と (カ) から s_1 とs_2 は $x_i+x_j+x_k$ (i, j, kは異なる) の形です.
さらに（ア）（エ）より「$f(-s_1-s_2)=0$」なので s_1 と s_2 は共通項 x_k を持ちません.
さらに (イ) (ウ) より $\{s_1, s_2, t_1, t_2\}$ =
$\{\sigma^i(x_1+x_2+x_4), \sigma^i(x_3+x_5+x_6), \sigma^i(r_1+r_2+r_4), \sigma^i(r_3+r_5+r_6)\}$ となります.

まず (ア) (イ) (ウ) から x, s_1, s_2 を消去すると

$$
\begin{cases} x=(t_1+t_2)/7 & \square \\ s_1=-(t_1+t_2)/14-\sqrt{-7}\,(t_1-t_2)/14 & \square \\ s_2=-(t_1+t_2)/14+\sqrt{-7}\,(t_1-t_2)/14 & \square \end{cases}
$$

これらを（エ）~ (カ) へ代入した後, f_3 と同様にt_1 の関係式 $(=G_1)$
とt_2 の関係式 $(=G_2)$ を求めることができますが,
更に「$f^+(x, y)=f_1(x)+f_2(y)$, $f^-(x, y)=\sqrt{-7}\,(f_1(x)-f_2(y))$」
を用いた方が効率的です.
(原論文によると, このまま計算すると約30秒かかるが, f^+, f^- を使うと 約3秒でできるそうです.)

「$f_1(s_1)=f_2(s_2)=0$」⇔「$f^+(s_1, s_2)=f^-(s_1, s_2)=0$」 ですから, （エ） (オ) (カ) より

$$
(\sharp 3)\quad f\left(\frac{t_1+t_2}{7}\right)=0\wedge f^+\left(-\frac{t_1+t_2}{14}-\frac{\sqrt{-7}\,(t_1-t_2)}{14},\ -\frac{t_1+t_2}{14}+\frac{\sqrt{-7}\,(t_1-t_2)}{14}\right)=
$$
$$
0\wedge f^-\left(-\frac{t_1+t_2}{14}-\frac{\sqrt{-7}\,(t_1-t_2)}{14},\ -\frac{t_1+t_2}{14}+\frac{\sqrt{-7}\,(t_1-t_2)}{14}\right)=0
$$

但し, $f^+(x, y)=f_1(x)+f_2(y)$, $f^-(x, y)=\sqrt{-7}\,(f_1(x)-f_2(y))$

この連立方程式を満たす t_1 の条件式が G_1 で, t_2 の条件式が G_2 です.
よって f_3 の時と同様, 終結式と最大公約因数（GCD）を用いて求まります.

（♯4）終結式と最大公約因数（GCD）を用いた求め方

$f\left(\frac{t_1+t_2}{7}\right)$ と $f^{+}\left(-\frac{t_1+t_2}{14}-\frac{\sqrt{-7}\,(t_1-t_2)}{14},\ -\frac{t_1+t_2}{14}+\frac{\sqrt{-7}\,(t_1-t_2)}{14}\right)$

の $\mathbf{t_2}$ に関する終結式 を$R1(t_1)$,

$f\left(\frac{t_1+t_2}{7}\right)$ と $f^{-}\left(-\frac{t_1+t_2}{14}-\frac{\sqrt{-7}\,(t_1-t_2)}{14},\ -\frac{t_1+t_2}{14}+\frac{\sqrt{-7}\,(t_1-t_2)}{14}\right)$

の $\mathbf{t_2}$ に関する終結式 を$R2(t_1)$

とすると，「$G1(t_1) = DCG(R1(t_1), R2(t_1))$」．G2 は R1, R2を「$\mathbf{t_1}$ に関する終結式」として求め「$G2(t_2) = DCG(R1(t_2), R2(t_2))$」

■ 例．$f(x) = x^7 + 4\,x^4 + x^3 - 2\,x^2 + 2\,x + 3$

まずは F1F2F3 . nb に挙げたコマンド findF12 を使って f1, f2を求めます．

In[195]:=

```
findF12[f_] := Module[{f35, factors, pos1, pos2, f12, f12listed},
 f35 = F35 /. AssociationThread[
     {a1, a2, a3, a4, a5, a6, a7} → Reverse@CoefficientList[f, x, 7]];
 factors = FactorList[f35];
 pos1 = Position[Exponent[factors〚All, 1〛, x], 14]〚1, 1〛;
 f12 = factors〚pos1〛〚1〛;
 d = Sqrt@Discriminant[f12, x];
 f12listed = FactorList[f12, Extension → d];
 pos2 = Flatten@Position[Exponent[f12listed〚All, 1〛, x], 7];
 (Expand[# / Coefficient[#, x, 7]] &) /@ f12listed
[[pos2]]〚All, 1〛
 ]
```

In[196]:=

```
f[x_] = x^7 + 4 x^4 + x^3 - 2 x^2 + 2 x + 3;
f12 = findF12[f[x]];
f1[x_] = f12〚1〛
f2[x_] = f12〚2〛
```

Out[198]=

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

Out[199]=

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

これらに対して $f^{+}(x, y)$ と $f^{-}(x, y)$ を作ります．なお Mathematicaの仕様上，f^{+}, f^{-} をそれぞれ fp, fm と表します．

In[200]:=

```
fp[x_, y_] := f1[x] + f2[y]
fm[x_, y_] := Sqrt[-7] (f1[x] - f2[y])
```

(#4) に従い， 次の様にg1 (x) が求まります． （最後の行は monic に直して， 変数を t1 → x に変えているだけです． なお実行時間は 4.25 秒でした .)

In[202]:=

```
R1 = Resultant[f[(t1 + t2) / 7], fp[
    - (t1 + t2) / 14 - Sqrt[-7] (t1 - t2) / 14, - (t1 + t2) / 14 + Sqrt[-7] (t1 - t2) / 14], t2];
R2 = Resultant[f[(t1 + t2) / 7], fm[
    - (t1 + t2) / 14 - Sqrt[-7] (t1 - t2) / 14, - (t1 + t2) / 14 + Sqrt[-7] (t1 - t2) / 14], t2];
gcd1 = PolynomialGCD[R1, R2, Extension → Automatic]
g1[x_] = Expand[gcd1 / Coefficient[gcd1, t1, 7]] /. {t1 → x}
```

Out[204]=

$$-237\,699 + 9261\sqrt{1057} + 61\,740\,t1 - 4116\sqrt{1057}\,t1 - 20\,580\,t1^2 + 1372\sqrt{1057}\,t1^2 + 3773\,t1^3 - 147\sqrt{1057}\,t1^3 - 882\,t1^4 + 14\sqrt{1057}\,t1^4 - 2\,t1^7$$

Out[205]=

$$\frac{237\,699}{2} - \frac{9261\sqrt{1057}}{2} - 30\,870\,x + 2058\sqrt{1057}\,x + 10\,290\,x^2 - 686\sqrt{1057}\,x^2 - \frac{3773\,x^3}{2} + \frac{147\sqrt{1057}\,x^3}{2} + 441\,x^4 - 7\sqrt{1057}\,x^4 + x^7$$

同様に g2 (x) が求まります.

In[206]:=

```
R1 = Resultant[f[(t1 + t2) / 7], fp[
    - (t1 + t2) / 14 - Sqrt[-7] (t1 - t2) / 14, - (t1 + t2) / 14 + Sqrt[-7] (t1 - t2) / 14], t1];
R2 = Resultant[f[(t1 + t2) / 7], fm[
    - (t1 + t2) / 14 - Sqrt[-7] (t1 - t2) / 14, - (t1 + t2) / 14 + Sqrt[-7] (t1 - t2) / 14], t1];
gcd2 = PolynomialGCD[R1, R2, Extension → Automatic];
g2[x_] = Expand[gcd2 / Coefficient[gcd2, t2, 7]] /. {t2 → x}
```

Out[209]=

$$\frac{237\,699}{2} + \frac{9261\sqrt{1057}}{2} - 30\,870\,x - 2058\sqrt{1057}\,x + 10\,290\,x^2 + 686\sqrt{1057}\,x^2 - \frac{3773\,x^3}{2} - \frac{147\sqrt{1057}\,x^3}{2} + 441\,x^4 + 7\sqrt{1057}\,x^4 + x^7$$

g1, g2を両方求めるには 約 4.25*2 = 8.5 秒 かかりましたが, 次のグレブナー基底を使うともっと速く求まります.

§2-3. グレブナー基底を使った求め方(原論文にはありません)

g1を求めるには(#3) の生成するイデアルのグレブナー基底を t2 を消去するモードで実行します.

In[210]:=

```
GroebnerBasis[{f[(t1 + t2) / 7],
  f1[-(t1 + t2) / 14 - Sqrt[-7] (t1 - t2) / 14] + f2[-(t1 + t2) / 14 + Sqrt[-7] (t1 - t2) / 14],
  Sqrt[-7] (f1[-(t1 + t2) / 14 - Sqrt[-7] (t1 - t2) / 14] -
     f2[-(t1 + t2) / 14 + Sqrt[-7] (t1 - t2) / 14])}, {t1}, {t2}]
Expand[# / Coefficient[#, t1, 7]] &[%[[1]]] /. {t1 → x}
```

Out[210]=

$$\left\{237699 - 9261\sqrt{1057} + \left(-61740 + 4116\sqrt{1057}\right) t1 + \left(20580 - 1372\sqrt{1057}\right) t1^2 + \left(-3773 + 147\sqrt{1057}\right) t1^3 + \left(882 - 14\sqrt{1057}\right) t1^4 + 2\, t1^7\right\}$$

Out[211]=

$$\frac{237699}{2} - \frac{9261\sqrt{1057}}{2} - 30870\, x + 2058\sqrt{1057}\, x + 10290\, x^2 - 686\sqrt{1057}\, x^2 - \frac{3773\, x^3}{2} + \frac{147\sqrt{1057}\, x^3}{2} + 441\, x^4 - 7\sqrt{1057}\, x^4 + x^7$$

g2を求めるには (#3) の生成するイデアルのグレブナー基底を t1 を消去するモードで実行します.

In[212]:=

```
GroebnerBasis[{f[(t1 + t2) / 7],
  f1[-(t1 + t2) / 14 - Sqrt[-7] (t1 - t2) / 14] + f2[-(t1 + t2) / 14 + Sqrt[-7] (t1 - t2) / 14],
  Sqrt[-7] (f1[-(t1 + t2) / 14 - Sqrt[-7] (t1 - t2) / 14] -
     f2[-(t1 + t2) / 14 + Sqrt[-7] (t1 - t2) / 14])}, {t2}, {t1}]
Expand[# / Coefficient[#, t2, 7]] &[%[[1]]] /. {t2 → x}
```

Out[212]=

$$\left\{237699 + 9261\sqrt{1057} + \left(-61740 - 4116\sqrt{1057}\right) t2 + \left(20580 + 1372\sqrt{1057}\right) t2^2 + \left(-3773 - 147\sqrt{1057}\right) t2^3 + \left(882 + 14\sqrt{1057}\right) t2^4 + 2\, t2^7\right\}$$

Out[213]=

$$\frac{237699}{2} + \frac{9261\sqrt{1057}}{2} - 30870\, x - 2058\sqrt{1057}\, x + 10290\, x^2 + 686\sqrt{1057}\, x^2 - \frac{3773\, x^3}{2} - \frac{147\sqrt{1057}\, x^3}{2} + 441\, x^4 + 7\sqrt{1057}\, x^4 + x^7$$

実行時間は各々0.8 秒程度なので, 合計でも約1.6 秒です. この方がずーと速いですが, グレブナー基底は時々予測不能の式を出してくるので, 少し心配ではあります. 実際, 少数ですが, うまくいかない例があります. (g1={t1}またはg2={t2}となります.) しかし, 通常はグレブナー基底による方法が速いので, それが上手くいかない場合のみに終結式を使うことにします.

(#5) グレブナー基底を使った求め方
g1を求めるには, (#3)の生成するイデアルのグレブナー基底を **t2 を消去するモード**で求める. g2を求めるには, **t1 を消去するモード**で求める. しかし上手くいかないことも稀にある.

§3. f1,f2,f3,g1, g2 を求めるプログラム

「findF1F2F3 . nb」と(#5) の方法を組み合わせると, Gal= F_{42}または D_7 のとき, fから f1, f2, f3, g1, g2 を求めるプログラムが作れます. ただし f3は不要なことが多いので, 別のプログラムとしています.

In[214]:=

```
findF12G12[f_] := Module[{f35, factors, pos1, pos2, f12, d,R1,R2, f12factors,u,v,fp,fm,g1,g2,g
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];
  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];
  {$f1,$f2}=(Expand[#/Coefficient[#, x, 7]] &) /@f12factors⟦pos2⟧⟦All, 1⟧;
  u=-(t1+t2)/14+(t1-t2)/(2Sqrt[-7]);
  v=-(t1+t2)/14-(t1-t2)/(2Sqrt[-7]);
 fp=($f1/.{x→u})+($f2/.{x→v});
 fm=Sqrt[-7](($f1/.{x→u})-($f2/.{x→v}));
g1=GroebnerBasis[{f/.{x→(t1+t2)/7},fp,fm},{t1},{t2}]⟦1⟧;
$g1=If[Coefficient[g1,t1,7]=!=0,Expand[#/Coefficient[#,t1,7]]&[g1]/.{t1→x},
R1=Resultant[f/.{x→(t1+t2)/7},fp/.{u→-(t1+t2)/14-Sqrt[-7](t1-t2)/14,v→-(t1+t2)/14+Sqrt[-7]
 R2=Resultant[f/.{x→(t1+t2)/7},fm/.{u→-(t1+t2)/14-Sqrt[-7](t1-t2)/14,v→-(t1+t2)/14+Sqrt[-7]
 PolynomialGCD[R1,R2,Extension→Automatic];
gcd1=PolynomialGCD[R1,R2,Extension→Automatic];
Expand[gcd1/Coefficient[gcd1,t1,7]]/.{t1→x}];
g2=GroebnerBasis[{f/.{x→(t1+t2)/7},fp,fm},{t2},{t1}]⟦1⟧;
$g2=If[Coefficient[g2,t2,7]=!=0,Expand[#/Coefficient[#,t2,7]]&[g2]/.{t2→x},
R1=Resultant[f/.{x→(t1+t2)/7},fp/.{u→-(t1+t2)/14-Sqrt[-7](t1-t2)/14,v→-(t1+t2)/14+Sqrt[-7]
 R2=Resultant[f/.{x→(t1+t2)/7},fm/.{u→-(t1+t2)/14-Sqrt[-7](t1-t2)/14,v→-(t1+t2)/14+Sqrt[-7]
 gcd2=PolynomialGCD[R1,R2,Extension→Automatic];
Expand[gcd2/Coefficient[gcd2,t2,7]]/.{t2→x}];
If[$g1===x^7,{$f1,$f2,$g1,$g2}={$f2,$f1,$g2,$g1}];
Return[{$f1,$f2,$g1,$g2}]]

(*findF3は$f1,$f2が必要なので, findF12G12が既に実行されている事が必要*)
findF3[f_]:=Module[{R1,R2,gcd3},
R1=Resultant[f,$f1/.{x→(t-x)/2},x];
 R2=Resultant[f,$f2/.{x→(-t-x)/2},x];
 gcd3=PolynomialGCD[R1,R2,Extension→Automatic];
 $f3=(Expand[#/Coefficient[#,t,7]]&[gcd3])/.{t→x}]
```

「$f = x^7 + 4x^4 + x^3 - 2x^2 + 2x + 3$」について , f1, f2, g1, g2 , f3 を, 実行時間と共に求めてみます. findF12G12, findF3 の出力は, それぞれ {f1, f2, g1, g2} と, f3 です. Global変数 $f1, $f2, $g1, $g2, $f3 も作ります.

In[216]:=

```
f[x_] = x^7 + 4 x^4 + x^3 - 2 x^2 + 2 x + 3;
Timing[findF12G12[f[x]]]
Timing[findF3[f[x]]]
```

Out[217]=

$$\left\{0.96875, \left\{-\frac{19}{2} - \frac{i\sqrt{151}}{2} + \frac{7x^3}{2} - \frac{3}{2} i\sqrt{151}\, x^3 + 5x^4 - i\sqrt{151}\, x^4 + x^7,\right.\right.$$
$$-\frac{19}{2} + \frac{i\sqrt{151}}{2} + \frac{7x^3}{2} + \frac{3}{2} i\sqrt{151}\, x^3 + 5x^4 + i\sqrt{151}\, x^4 + x^7,$$
$$\frac{237699}{2} - \frac{9261\sqrt{1057}}{2} - 30870x + 2058\sqrt{1057}\, x + 10290x^2 - 686\sqrt{1057}\, x^2 - \frac{3773x^3}{2} +$$
$$\frac{147\sqrt{1057}\, x^3}{2} + 441x^4 - 7\sqrt{1057}\, x^4 + x^7,\ \frac{237699}{2} + \frac{9261\sqrt{1057}}{2} - 30870x - 2058\sqrt{1057}\, x +$$
$$\left.\left.10290x^2 + 686\sqrt{1057}\, x^2 - \frac{3773x^3}{2} - \frac{147\sqrt{1057}\, x^3}{2} + 441x^4 + 7\sqrt{1057}\, x^4 + x^7\right\}\right\}$$

Out[218]=

$$\left\{0.6875, -41 i\sqrt{151} + 6x + 42 i\sqrt{151}\, x^2 - 35x^3 - 8 i\sqrt{151}\, x^4 + x^7\right\}$$

F35から始まり長~い考察を経て，やっと「f1, f2, f3, g1, g2 が全て合わせても 2秒程度」で求まるようになりました．(^^)/

解の公式には, これ以外の関数は必要ありません.

§4. g1, g2 ,f1+f2, $\sqrt{D}$ (f1-f2)の係数の体

g1, g2 は F_{21} によって不変で, その定義に ζ を含むので ,その係数は Q(ζ, $\sqrt{D}$) (Dはfの判別式)に属しますが, 実は Q($\sqrt{-7D}$)に属します. まず $\sqrt{D}$ が有理数でない時,「f_1(x) =h(x)+g(x) $\sqrt{D}$, f_2(x) =h(x)-g(x) $\sqrt{D}$ (h,gの係数は有理数)」の様になります. 例えば§3の例の f1, f2 で確認できます.

In[219]:=

```
$f1
$f2
Discriminant[f[x], x] // Sqrt(* √判別式 *)
```

Out[219]=

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

Out[220]=

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

Out[221]=

$$1359\,i\sqrt{151}$$

次に（t_1+t_2）/（−14）= u, （t_1-t_2）/（−14）= v とおき, （♯3）の条件を書き直すと

(a) $f^{+}\left(-\frac{t_1+t_2}{14}-\frac{\sqrt{-7}\,(t_1-t_2)}{14},\ -\frac{t_1+t_2}{14}+\frac{\sqrt{-7}\,(t_1-t_2)}{14}\right)=$

$f^{+}\left(u+\sqrt{-7}\,v,\ u-\sqrt{-7}\,v\right)=f_1\left(u+\sqrt{-7}\,v\right)+f_2\left(u-\sqrt{-7}\,v\right)=$
$\left\{h\left(u+\sqrt{-7}\,v\right)+h\left(u-\sqrt{-7}\,v\right)\right\}+\left\{g\left(u+\sqrt{-7}\,v\right)-g\left(u-\sqrt{-7}\,v\right)\right\}\sqrt{D}$

(b) $f^{-}\left(-\frac{t_1+t_2}{14}-\frac{\sqrt{-7}\,(t_1-t_2)}{14},\ -\frac{t_1+t_2}{14}+\frac{\sqrt{-7}\,(t_1-t_2)}{14}\right)=$

$f^{-}\left(u+\sqrt{-7}\,v,\ u-\sqrt{-7}\,v\right)=\sqrt{-7}\left(f_1\left(u+\sqrt{-7}\,v\right)-f_2\left(u-\sqrt{-7}\,v\right)\right)=$
$\sqrt{-7}\left\{h\left(u+\sqrt{-7}\,v\right)-h\left(u-\sqrt{-7}\,v\right)\right\}+\sqrt{-7D}\left\{g\left(u+\sqrt{-7}\,v\right)+g\left(u-\sqrt{-7}\,v\right)\right\}$

h(x), g(x)は有理数係数の整式なので「$h\left(u+\sqrt{-7}\,v\right)+h\left(u-\sqrt{-7}\,v\right)=H_1(u,v)$, $h\left(u+\sqrt{-7}\,v\right)-h\left(u-\sqrt{-7}\,v\right)=\sqrt{-7}\,H_2(u,v)$, $g\left(u+\sqrt{-7}\,v\right)+g\left(u-\sqrt{-7}\,v\right)=G_1(u,v)$, $g\left(u+\sqrt{-7}\,v\right)-g\left(u-\sqrt{-7}\,v\right)=\sqrt{-7}\,G_2(u,v)$ （H_i, G_i は有理数係数の整式)」となり, (a) は「$H_1(u,v)+\sqrt{-7D}\,G_2(u,v)=p_1(t_1,t_2)+\sqrt{-7D}\,p_2(t_1,t_2)$ 」, (b)は「$-7H_2(u,v)+\sqrt{-7D}\,G_1(u,v)=p_3(t_1,t_2)+\sqrt{-7D}\,p_4(t_1,t_2)$ 」(p_i は有理数係数の整式) となります.

故に終結式の性質（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（$\sqrt{-7D}$）に入るので, そのGCDである g_1, g_2 の係数も Q（$\sqrt{-7D}$）に入ります. 例えば, 先の f（x）では「$\sqrt{-7D}=\sqrt{7}\,i*1359\,i\sqrt{151}=1359\sqrt{1057}$」ですから, 係数はQ（$\sqrt{1057}$）に入ります. 実際に見てみると, 確かにそうなっています.

In[222]:=

```
$g1
$g2
```

Out[222]=

$$\frac{237699}{2}-\frac{9261\sqrt{1057}}{2}-30870x+2058\sqrt{1057}x+10290x^2-686\sqrt{1057}x^2-\frac{3773x^3}{2}+\frac{147\sqrt{1057}x^3}{2}+441x^4-7\sqrt{1057}x^4+x^7$$

Out[223]=

$$\frac{237699}{2}+\frac{9261\sqrt{1057}}{2}-30870x-2058\sqrt{1057}x+10290x^2+686\sqrt{1057}x^2-\frac{3773x^3}{2}-\frac{147\sqrt{1057}x^3}{2}+441x^4+7\sqrt{1057}x^4+x^7$$

f の判別式を D とすると，g_1，g_2 の係数の体は $Q\left(\sqrt{-7D}\right)$ に含まれる

また「$f_1(x)=h(x)+g(x)\sqrt{D}$，
$f_2(x)=h(x)-g(x)\sqrt{D}$ (h，gの係数は有理数)」となることから

$f_1(x)+f_2(x)$，$\sqrt{D}(f_1(x)-f_2(x))$ の係数は 有理数

となります．