解の公式 その1 (r_1, r_2, r_4 を求める) with Mathematica14.0

§0 準備

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

F35↓（評価してください)

```
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}]
```

§1. r_1, r_2, r_4 の関係式

定義より

In[∘]:=
```
G1 = (x - (r1 + r2 + r4)) (x - (ξ r1 + ξ ^2 r2 + ξ ^4 r4)) (x - (ξ^2 r1 + ξ ^4 r2 + ξ r4))
    (x - (ξ^3 r1 + ξ ^6 r2 + ξ ^5 r4)) (x - (ξ^4 r1 + ξ r2 + ξ ^2 r4))
    (x - (ξ^5 r1 + ξ ^3 r2 + ξ ^6 r4)) (x - (ξ^6 r1 + ξ ^5 r2 + ξ ^3 r4));
```

これを「$1 + \xi + \xi^2 + \cdots + \xi^6 = 0$」を使って変形すると,

In[∘]:=
```
G1 = PolynomialMod[G1, Cyclotomic[7, ξ]] // Collect[#, x] & // Simplify
```

Out[∘]=

$$-r1^7 - r2^7 - 7\, r1^2\, r2^4\, r4 - 7\, r1^4\, r2\, r4^2 - 7\, r1\, r2^2\, r4^4 - r4^7 - 7\left(r1^5\, r2 + r2^5\, r4 + r1^2\, r2^2\, r4^2 + r1\, r4^5\right) x - 14\left(r1^3\, r2^2 + r2^3\, r4^2 + r1^2\, r4^3\right) x^2 - 7\left(r1\, r2^3 + r1^3\, r4 + r2\, r4^3\right) x^3 - 14\, r1\, r2\, r4\, x^4 + x^7$$

これと $x^7 + b_1 x^6 + b_2 x^5 + b_3 x^4 + b_4 x^3 + b_5 x^2 + b_6 x + b_7$ と比べて少し変形すると「$b_1 = b_2 = 0$」かつ以下の式が成り立ちます.

$$(\#)\quad \begin{cases} r_1 r_2 r_4 = -b_3 / 14 & (6) \\ r_1 {r_2}^3 + r_2 {r_4}^3 + r_4 {r_1}^3 = -b_4 / 7 & (7) \\ {r_1}^3 {r_2}^2 + {r_2}^3 {r_4}^2 + {r_4}^3 {r_1}^2 = -b_5 / 14 & (8) \\ {r_1}^5 r_2 + {r_2}^5 r_4 + {r_4}^5 r_1 = -b_6 / 7 - {b_3}^2 / 197 & (9) \\ {r_1}^7 + {r_2}^7 + {r_4}^7 = -b_7 - b_3 b_4 / 14 & (10) \end{cases}$$

§2. r_1,r_2,r_4 を求める公式(b_3≠0 のとき)

「b_3≠0 のとき」としてありますが，下の公式の(13)(14)以外は「b_3=0 のとき」も成り立ちます．さて(#)の生成するイデアルのグレブナー基底を作り r_2, r_4 を r_1 の式で表します．原論文ではMapleを使っていて(かつMapleのグレブナー基底はMathematicaのより高機能の様なので) それを厳密に再現することはできませんでした．例えば，原論文では，「b_3=0」の時は (tb_3-1)を(#)に加えたイデアルのt を消去したグレブナー基底を作り(1.5秒)，それから更に r_4 を消去しているようですが，私は初めから r_4 を消去しました．その計算は2分ほど掛かるので，下のコマンドはテキスト形式で，結果はclosed cell に入れてあります．

gb = GroebnerBasis[{ r1 r2 r4 + b3/14, r1 r2^3 + r2 r4^3 + r4 r1^3 + b4/7, r1^3 r2^2 + r2^3 r4^2 + r4^3 r1^2 + b5/14, r1^5 r2 + r2^5 r4 + r4^5 r1 + b6/7 + b3^2/196, r1^7 + r2^7 + r4^7 + b7 + b3 b4/14}, {r2, r1, b7, b6, b5, b4, b3}, { r4}];(gbの結果は↓です．評価してください.)

gbは 209 個の式から成り立ちますが，最初の3式は b_1 ~ b_7 の関係式です．

In[ ]:=
```
gb[[1 ;; 3]]
```
Out[ ]=

$$\{b3^5 - 16\, b3\, b4^3 + 20\, b3^2\, b4\, b5 + 28\, b5^3 - 4\, b3^3\, b6 - 112\, b4\, b5\, b6 + 112\, b3\, b6^2,\ b3^2\, b4 + b5^2 - 4\, b4\, b6 + 14\, b3\, b7,\ -b3^4 + 16\, b4^3 + 8\, b3\, b4\, b5 + 4\, b3^2\, b6 - 112\, b6^2 + 392\, b5\, b7\}$$

b_1 ~ b_7 以外の変数を考えると，第4式は r_1 のみの式です．

In[ ]:=
```
gb[[4]] // Collect[#, {r1^7, r1^14}] &
```
Out[ ]=

$$b3^7 + (-10\,976\, b3^2\, b4^2 - 2744\, b3^3\, b5 - 76\,832\, b4\, b5^2 + 76\,832\, b3\, b5\, b6)\, r1^7 + (7\,529\,536\, b3\, b4 + 105\,413\,504\, b7)\, r1^{14} + 105\,413\,504\, r1^{21}$$

これから $r_1{}^7$ についての3次方程式が得られます．
また 第57式は r_1 とr_2 の式 かつ r_2 については1次ですから r_2 が r_1 の式で表せます．

In[ ]:=
```
gb[[57]] // Collect[#, {r1, r2}] &
```
Out[ ]=

$$(-2\, b3^6 + 56\, b3^2\, b4^3 - 56\, b3^3\, b4\, b5 + 392\, b4^2\, b5^2 - 196\, b3\, b5^3 - 14\, b3^4\, b6 - 392\, b3\, b4\, b5\, b6)\, r1^2 + (-10\,976\, b3\, b4^2 + 2744\, b3^2\, b5 - 38\,416\, b5\, b6)\, r1^9 + (-b3^5\, b4 + 28\, b3^2\, b4^2\, b5 - 14\, b3^3\, b5^2 - 28\, b3^3\, b4\, b6)\, r2 + (196\, b3^4 + 10\,976\, b4^3 - 2744\, b3\, b4\, b5 + 76\,832\, b6^2)\, r1^7\, r2$$

In[ ]:=
```
r2 /. Solve[% == 0, r2][[1]] (*r2をr1で表した式*)
```
Out[ ]=

$$-\left(\left(2\left(b3^6\, r1^2 - 28\, b3^2\, b4^3\, r1^2 + 28\, b3^3\, b4\, b5\, r1^2 - 196\, b4^2\, b5^2\, r1^2 + 98\, b3\, b5^3\, r1^2 + 7\, b3^4\, b6\, r1^2 + 196\, b3\, b4\, b5\, b6\, r1^2 + 5488\, b3\, b4^2\, r1^9 - 1372\, b3^2\, b5\, r1^9 + 19\,208\, b5\, b6\, r1^9\right)\right) \Big/ \left(b3^5\, b4 - 28\, b3^2\, b4^2\, b5 + 14\, b3^3\, b5^2 + 28\, b3^3\, b4\, b6 - 196\, b3^4\, r1^7 - 10\,976\, b4^3\, r1^7 + 2744\, b3\, b4\, b5\, r1^7 - 76\,832\, b6^2\, r1^7\right)\right)$$

故に，$R_1 = r_1{}^7$ とおくと，R_1 は次の3次方程式の解で，R_1 の7乗根である r_1 を決めると，
r_2，r_4 も決まります．また $r_2{}^7$，$r_4{}^7$ も同じ3次方程式の解です．

「$b_3 = b_4 = b_5 = b_6 = 0$ でない時」に r_1，r_2，r_4 を求める公式

$$R_1 = r_1{}^7 \tag{11}$$

$$R_1{}^3 + \left(\frac{b_3 b_4}{14} + b_7\right) R_1{}^2 + \left(-\frac{b_3{}^2 b_4{}^2}{9604} - \frac{b_3{}^3 b_5}{38416} - \frac{b_4 b_5{}^2}{1372} + \frac{b_3 b_5 b_6}{1372}\right) R_1 + \left(\frac{b_3}{14}\right)^7 = 0 \tag{12}$$

$$r_2 = -2 r_1{}^2 \cdot \frac{R_1 \left(5488 b_3 b_4{}^2 - 1372 b_3{}^2 b_5 + 19208 b_5 b_6\right) + A}{R_1 \left(-196 b_3{}^4 - 10976 b_4{}^3 + 2744 b_3 b_4 b_5 - 76832 b_6{}^2\right) + B} \tag{13}$$

$$r_4 = \frac{-b_3}{14 r_1 r_2} \tag{14}$$

$$A = b_3{}^6 - 28 b_3{}^2 b_4{}^3 + 28 b_3{}^3 b_4 b_5 - 196 b_4{}^2 b_5{}^2 + 98 b_3 b_5{}^3 + 7 b_3{}^4 b_6 + 196 b_3 b_4 b_5 b_6 \quad \square$$

$$B = b_3{}^5 b_4 - 28 b_3{}^2 b_4{}^2 b_5 + 14 b_3{}^3 b_5{}^2 + 28 b_3{}^3 b_4 b_6 \quad \square$$

適用条件で「$b_3 = b_4 = b_5 = b_6 = 0$ でない時」とありますがこれは後述します．
なおこの適用条件を満たす時（12）が重解を持たないことが言えるので（後述），
「（13）の分母と分子が共に0」となる時は，（12）の解を適切に取ることが出来ます．

§3. r_1,r_2,r_4 を求める公式(b_3=0 のとき)

「$b_3 = 0$」のときも（12）は成り立ちますが，「$b_3 = b_4 = 0$」のときは （13），（14）は不成立です．（6）より $r_1 r_2 r_4 = 0$．ここで $r_4 = 0$ としても一般性を失いません．このとき（7），（8），（9），（10）より

$$\begin{cases} r_1 r_2^3 = -b_4 / 7 & (7)' \\ r_1^3 r_2^2 = -b_5 / 14 & (8)' \\ r_1^5 r_2 = -b_6 / 7 & (9)' \\ r_1^7 + r_2^7 = -b_7 & (10)' \end{cases}$$

§3 - 1 $b_3 = b_4$=0 のとき

「$r_1 = 0$ または $r_2 = 0$」となるので「$b_3 = b_4 = b_5 = b_6 = 0$」となります．ここで「$r_2 = 0$」としても構いません．（10）' より $r_1^7 = -b_7$．故に $r_1 = \sqrt[7]{-b_7}$

「$b_7 = 0$ のときは $r_1 = 0$」となり「$r_2 \sim r_6$ を r_1 で表す」という目的に使えません．しかし，この時はτによって変換すると「$f_1 \leftrightarrow f_2$，$g_1 \leftrightarrow g_2$」となるから，この新しい g_1 で考えると（fが既約であることから）「$b_3 = b_4 = b_5 = b_6 = b_7 = 0$」となることはないです．

§3 - 2 b_3=0, b_4≠0 のとき

「（8）' × （9）' / （7）'」より「$r_1^7 = \dfrac{-b_5 b_6}{14 b_4}$」，

故に（A）「$r_1 = \sqrt[7]{\dfrac{-b_5 b_6}{14 b_4}}$」．　また（9）' より （B）「$r_2 = \dfrac{2 r_1^2 b_4}{b_5}$」

また，$b_3 = 0$ のとき（12）は「$R_1 = 0$」または　（C）「$R_1^2 + b_7 R_1 + \left(-\dfrac{b_4 b_5^2}{1372}\right)$」．ここで

「（7）' （9）' = （（8）'）^{2}」より「$b_5^2 = b_4 b_6$」．これを使うと
「r_1^7 と r_2^7 は（C）の2解である事」と「（13）と（B）が一致する事」が言えます．

故に，この場合は「$b_3 \neq 0$」の場合の公式（12），（13），（14）が成り立つことが分かります．
即ち「$b_3 \neq 0$」の場合に統合できます．（原論文では統合はせず，3 つに分けています）

§4 例を２つ

(12) の方程式を Rと置きます.

In[∘]:=
$$R = x^3 + \left(\frac{b_3\, b_4}{14} + b_7\right) x^2 + \left(-\frac{b_3^2\, b_4^2}{9604} - \frac{b_3^3\, b_5}{38\,416} - \frac{b_4\, b_5^2}{1372} + \frac{b_3\, b_5\, b_6}{1372}\right) x + \left(\frac{b_3}{14}\right)^7;$$

1. $f = x^7 - 2x^5 + x^4 + 4x^3 - x^2 - 4x + 3$ (Gal = F_{42})

まず, g1と {b3, b4, b5, b6, b7} を求めます

In[∘]:=
```
f = x^7 - 2 x^5 + x^4 + 4 x^3 - x^2 - 4 x + 3 ;
findF12G12[f];
g1 = %[[3]]
{b3, b4, b5, b6, b7} = CoefficientList[g1, x, 5] // Reverse
```

Out[∘]=
$$\frac{381\,759}{2} - \frac{108\,045\sqrt{13}}{2} - \frac{220\,549\,x}{2} + \frac{64\,827\sqrt{13}\,x}{2} + 20\,580\,x^2 - 6174\sqrt{13}\,x^2 - \frac{2401\,x^3}{2} + \frac{1029\sqrt{13}\,x^3}{2} + 196\,x^4 + x^7$$

Out[∘]=
$$\left\{196,\ -\frac{2401}{2} + \frac{1029\sqrt{13}}{2},\ 20\,580 - 6174\sqrt{13},\ -\frac{220\,549}{2} + \frac{64\,827\sqrt{13}}{2},\ \frac{381\,759}{2} - \frac{108\,045\sqrt{13}}{2}\right\}$$

次に Rとその解solを求めます

In[∘]:=
```
R /. AssociationThread[{b3, b4, b5, b6, b7} → {b3, b4, b5, b6, b7}] // Simplify
sol = x /. NSolve[% == 0, x]
```

Out[∘]=
$$105\,413\,504 - \frac{117\,649}{2}\left(-22\,501 + 6261\sqrt{13}\right) x - \frac{2401}{2}\left(-145 + 39\sqrt{13}\right) x^2 + x^3$$

Out[∘]=
{-5986.19, 25.2072, 698.588}

r_2 を求め易くするため (13) を関数にします.

```
findr2[r1_] :=
 Simplify[-2 (r1)^2 * ((r1^7 (5488 b3 b4^2 - 1372 b3^2 b5 + 19 208 b5 b6) + b3^6 - 28 b3^2 b4^3 +
        28 b3^3 b4 b5 - 196 b4^2 b5^2 + 98 b3 b5^3 + 7 b3^4 b6 + 196 b3 b4 b5 b6) /
      (r1^7 (-196 b3^4 - 10 976 b4^3 + 2744 b3 b4 b5 - 76 832 b6^2) + b3^5 b4 -
        28 b3^2 b4^2 b5 + 14 b3^3 b5^2 + 28 b3^3 b4 b6))]
```

「r_1 = sol[[1]]^(1/7)」の場合に r_2 と r_2^7 を求めます.

In[ ]:=
```
r1 = sol[[1]]^(1 / 7)
r2 = findr2[r1]
r2^7
```

Out[ ]=

3.12106 + 1.50303 i

Out[ ]=

0.988661 + 1.23974 i

Out[ ]=

$25.2072 - 3.55271 \times 10^{-15}\, i$

確かに「 $r_2{}^7$ も R = 0 の解の一つ（ = sol〚2〛）」となっています.

次に「r_1 = sol〚2〛^（1 / 7）」の場合に r_2 と $r_2{}^7$ を求めます.

In[ ]:=
```
r1 = sol[[2]]^(1 / 7)
r2 = findr2[r1]
r2^7
```

Out[ ]=

1.58569

Out[ ]=

2.54869

Out[ ]=

698.588

「$r_2{}^7$ = sol〚3〛」となっています. 最後に「r_1 = sol〚3〛^（1 / 7）」の場合に r_2 と $r_2{}^7$ を求めます.

In[ ]:=
```
r1 = sol[[3]]^(1 / 7)
r2 = findr2[r1]
r2^7
```

Out[ ]=

2.54869

Out[ ]=

-3.46412

Out[ ]=

-5986.19

「$r_2{}^7$ = sol〚1〛」となっています.

2. $f = x^7 - 7x^5 + 14x^3 - 7x + 3$ (Gal = F_{42})

まず, g1と {b3, b4, b5, b6, b7} を求めます

In[∘]:=
```
f = f = x^7 - 7 x^5 + 14 x^3 - 7 x + 3;
findF12G12[f];
g1 = %[[3]]
{b3, b4, b5, b6, b7} = CoefficientList[g1, x, 5] // Reverse
```

Out[∘]=

$$\frac{2470629}{2} + \frac{823543\sqrt{5}}{2} + x^7$$

Out[∘]=

$$\left\{0, 0, 0, 0, \frac{2470629}{2} + \frac{823543\sqrt{5}}{2}\right\}$$

次に Rとその解solを求めます

In[∘]:=
```
R /. AssociationThread[{b3, b4, b5, b6, b7} → {b3, b4, b5, b6, b7}] // Simplify
sol = x /. NSolve[% == 0, x]
```

Out[∘]=

$$\frac{823543}{2}\left(3 + \sqrt{5}\right) x^2 + x^3$$

Out[∘]=

$$\{-2.15606 \times 10^6, 0., 0.\}$$

「r_1 = sol[[1]]^(1/7) ζ^k ($0 \le k \le 6$)」です.
また (13), (14) の式は使えませんが「$r_2 = r_4 = 0$」です.

In[∘]:=
```
ζ = Cos[2 Pi / 7] + I Sin[2 Pi / 7];
```

In[∘]:=
```
r1 = sol[[1]]^(1 / 7) × Table[ζ^k, {k, 0, 6}]
```

Out[∘]=

$$\{7.23633 + 3.48483\,i, 1.78723 + 7.83035\,i, -5.0077 + 6.27945\,i, -8.03172 - 4.44089 \times 10^{-16}\,i, -5.0077 - 6.27945\,i, 1.78723 - 7.83035\,i, 7.23633 - 3.48483\,i\}$$

最終的にはこれらの r_1 の値のうち, 適切なものを数値計算などを使って選ぶ必要があります.

§5. 式(12)の判別式

式 (12) の判別式をDとすると , D は 次のd の平方と一致する事
, 更に「$b_3 = b_4 = b_5 = b_6 = 0$」のときに限り「$d = 0$」となる事 が証明できます.

【命題14】

$$d = \frac{b_5^2\, b_4^2\, b_3}{7^3 \times 14^2} - \frac{b_5^3\, b_3^2}{14^5} - \frac{b_6\, b_5\, b_4\, b_3^2}{7^4 \times 14} + \frac{b_3^7}{14^7} - \frac{b_4^4\, b_5}{7^4 \times 14} - \frac{b_6\, b_5^3}{7 \times 14^3} - \frac{b_3^3\, b_4^3}{7^4 \times 14^2} + \frac{3\, b_5\, b_4\, b_3^4}{7 \times 14^5} - \frac{b_6\, b_3^5}{14^4 \times 7^2} + \frac{b}{}$$

更に「$b_3 = b_4 = b_5 = b_6 = 0$」のときに限り「$d = 0$」となる

§5 - 1【命題14】の前半の証明

原論文では グレブナー基底を使って次の様に証明しています.

First compute the Grobner basis G1 of Equations 6 to 10 for an elimination ordering eliminating the r_i (1 / 3 second in MAPLE for the ordering lexdeg ([r1, r2, r4], [b3, b4, b5, b6, b7], method = fgb) and the Grobner basis G2 of the elements of G1 which depend only on b3, b4, b5, b6, b7, for the lexicographical ordering such that b7 > b6 > b5 > b4 > b3. Then Polynomial (15) is obtained by taking the normal form by G2 of the normal form by G1 of $(r1^7 - r_2^7)\ (r_2^7 - r_4^7)\ (r_4^7 - r_1^7)$.

しかし, 残念ながらこの通りにはできず, r_4 を消去して導きました. 先ず r_1^7, r_2^7, r_4^7 は (12) の解なので「$d = (r_1^7 - r_2^7)\ (r_2^7 - r_4^7)\ (r_4^7 - r_1^7)$」とおくと, $D = d^2$ です. 式 (10) を使って $d から r_4 を消去します.

In[ ]:=
```
Clear[r1, r2, r4, b3, b4, b5, b6, b7]
```

In[ ]:=
```
$d = (r1^7 - r2^7) (r2^7 - r4^7) (r4^7 - r1^7) /.
    {r4^7 → - b7 - b3 b4 / 14 - r1^7 - r2^7} // Expand // Simplify
```

Out[ ]=

$$-\frac{1}{196}\ (r1^7 - r2^7)\ \left(b3^2\, b4^2 + 14\, b3\, b4\, \left(2\, b7 + 3\, (r1^7 + r2^7)\right) + 196\, \left(b7^2 + 2\, r1^{14} + 5\, r1^7\, r2^7 + 2\, r2^{14} + 3\, b7\, (r1^7 + r2^7)\right)\right)$$

この $d を gb を使って簡約します. Mathematicaでは「簡約」は「 PolynomialReduce」です.

In[ ]:=

PolynomialReduce[$poly$, {$poly_1$, $poly_2$, …}, {x_1, x_2, …}]
$poly_i$ によって $poly$ を簡約したリストを返す. 求まるリストは {{a_1, a_2, …}, b} の形であり, b は最小で, $poly$ は $a_1\ poly_1 + a_2\ poly_2 + \ldots + b$ に等しい.

In[ ]:=
```
[例] f = x^3 + y^3;
p = {x^2 - y^2 - 1, x + 2 y - 7};
PolynomialReduce[f, p, {x, y}]
```

$$\{\{x,\ 1+y^2\},\ 7-2y+7y^2-y^3\}$$

In[∘]:=
```
$d = PolynomialReduce[$d, gb, {r2, r1, b7, b6, b5, b4, b3}][[2]] // Expand
```

Out[∘]=

$$\frac{b3^7}{105\,413\,504}-\frac{b3^3\,b4^3}{470\,596}+\frac{3\,b3^4\,b4\,b5}{3\,764\,768}-\frac{b4^4\,b5}{33\,614}+\frac{b3\,b4^2\,b5^2}{67\,228}-\frac{b3^2\,b5^3}{537\,824}-\frac{b3^5\,b6}{1\,882\,384}+\frac{b3\,b4^3\,b6}{33\,614}-\frac{b3^2\,b4\,b5\,b6}{33\,614}-\frac{b5^3\,b6}{19\,208}$$

確かに $D = d^2$ となっています.

§5 - 2 $R_1(=r_1{}^7)$の体

1. (12) の3次方程式R が既約のとき

一般に　係数の体がKで，既約な3次方程式fの判別式Dが「$D = d^2$ （$d \in K$）」となっているとき，
fの解は $K\left(\sqrt{-3}\right)$ に入ります．g_1 の係数は $Q\left(\sqrt{-7D}\right)$ に入るので，
R_1 は $Q\left(\sqrt{-3},\ \sqrt{-7D}\right)$ に入ります.

2. (12) の3次方程式R が (2次式)と(1次式)の積のとき

1 次式を「$h1 = x + p$」，2 次式を「$h2 = x^2 + q\,x + r$」と置くと，
「$\left(h1 \times h2\text{の判別式 } D\right) = \left(h2\text{の判別式}\right)\left(h1\text{と}h2\text{の終結式}\right)^2$」が成り立ちます．（下を参照）

In[∘]:=
```
h1 = x + p;
h2 = x^2 + q x + r;
Discriminant[h1 h2, x]
Resultant[h1, h2, x]
```

Out[∘]=

$$\left(q^2-4r\right)\left(p^2-p\,q+r\right)^2$$

Out[∘]=

$$p^2-p\,q+r$$

よって「$D = d^2$」のとき，「h2の判別式 $= e^2$，$e \in Q\left(\sqrt{-7D}\right)$」となります.
従って h2 の解は $Q\left(\sqrt{-7D}\right)$ に入り，Rの解は全て $Q\left(\sqrt{-7D}\right)$ に入ります

これはR が 3 個の1次式の積の時も成り立つので，結局次のようになります.

【系15】3 次方程式（12）の解は　$Q\left(\sqrt{-3},\ \sqrt{-7D}\right)$ または $Q\left(\sqrt{-7D}\right)$ に入る

§5- 3【命題14】の後半の証明

「$b_3 = b_4 = b_5 = b_6 = 0$」でないが「$d = 0$」となったと仮定します． このとき r_1，r_2，r_4 のうち高々1個だけ0となるので「r_1，$r_2 \neq 0$」としても構いません．
このとき「$d = 0$」より「${r_1}^7 = {r_2}^7$」だから「$r_2 = r_1 \zeta$（ζは1の原始7乗根のひとつ）」です．

（6）へ代入して「$r_4 = -\dfrac{b_3}{14 {r_1}^2 \zeta}$」．さらにこれらを（7），
（8）へ代入し，右辺が0となるように移項したとき，
左辺の式をそれぞれh1，h2 とおくと， 共に r_1 の9次式となります．

In[∘]:=
```
ClearAll[r1, r2, r4, b3, b4, b5, b6, b7, ζ]
```

In[∘]:=
```
h1 = (r1 r2^3 + r2 r4^3 + r4 r1^3 /. {r2 → r1 ζ, r4 → -b3/(14 r1^2 ζ)}) + b4 / 7
```

Out[∘]=

$$\frac{b4}{7} - \frac{b3^3}{2744\, r1^5\, \zeta^2} - \frac{b3\, r1}{14\, \zeta} + r1^4\, \zeta^3$$

In[∘]:=
```
$h1 = h1 * 2744 r1^5 ζ^2 // Expand
```

Out[∘]=

$$-b3^3 - 196\, b3\, r1^6\, \zeta + 392\, b4\, r1^5\, \zeta^2 + 2744\, r1^9\, \zeta^5$$

In[∘]:=
```
h2 = (r1 ^3 r2^2 + r2^3 r4^2 + r4^3 r1^2 /. {r2 → r1 ζ, r4 → -b3/(14 r1^2 ζ)}) + b5 / 14
```

Out[∘]=

$$\frac{b5}{14} - \frac{b3^3}{2744\, r1^4\, \zeta^3} + \frac{b3^2\, \zeta}{196\, r1} + r1^5\, \zeta^2$$

In[∘]:=
```
$h2 = h2 * 2744 r1^4 ζ^3 // Expand
```

Out[∘]=

$$-b3^3 + 196\, b5\, r1^4\, \zeta^3 + 14\, b3^2\, r1^3\, \zeta^4 + 2744\, r1^9\, \zeta^5$$

In[∘]:=
```
$h1 - $h2
```

Out[∘]=

$$-196\, b3\, r1^6\, \zeta + 392\, b4\, r1^5\, \zeta^2 - 196\, b5\, r1^4\, \zeta^3 - 14\, b3^2\, r1^3\, \zeta^4$$

更に${r_1}^3$ で（$h1 - $h2）を割ると r_1 の3次式となるので，
r_1 は $Q\left(\sqrt{-7D}, \zeta\right)$ 係数の3次方程式の解となります．これは【系15】と矛盾するから，
「$d = 0$」となるのは「$b_3 = b_4 = b_5 = b_6 = 0$」のときに限ります．