分解方程式，原始元，ガロア群 の基本 with *Mathematica* 13.3

2025 年2月　by　mixedmoss

§1.　分解方程式の作成

Galois 分解方程式を求めるには　色々方法があると思いますが，ここでは「数学の教科書に載っている方法」と「Grobner基底による方法」の2つを Mathematica でプログラムしたのでご紹介します．例として，４次関数 $f(x) = x^4 - 10x^2 + 1$ を取り上げます．

---

§1 -A. 対称性の利用(参考文献[7][8]の方法)

In[1]:=
```
ClearAll["`*"];

f[x_] = x^4 - 10 x^2 + 1;
x /. Solve[f[x] == 0, x] (*f(x)=0の解*)
```

Out[3]=
$$\left\{-\sqrt{5-2\sqrt{6}},\ \sqrt{5-2\sqrt{6}},\ -\sqrt{5+2\sqrt{6}},\ \sqrt{5+2\sqrt{6}}\right\}$$

f[x] = 0 の解を $\{\alpha, \beta, \gamma, \delta\}$ とする．同じ値がないように vs を取る．（下の係数は{1,3,-1,0}ですが，vsの中に同じ「値」がなければ何でも大丈夫です．もし同じ値があれば，次のR(x)が重解を持つので分かります．）

In[4]:=
```
vs = Permutations[{α, β, γ, δ}].{1, 3, -1, 0}
```

Out[4]=
$$\{\alpha+3\beta-\gamma,\ \alpha+3\beta-\delta,\ \alpha-\beta+3\gamma,\ \alpha+3\gamma-\delta,\ \alpha-\beta+3\delta,\ \alpha-\gamma+3\delta,$$
$$3\alpha+\beta-\gamma,\ 3\alpha+\beta-\delta,\ -\alpha+\beta+3\gamma,\ \beta+3\gamma-\delta,\ -\alpha+\beta+3\delta,\ \beta-\gamma+3\delta,$$
$$3\alpha-\beta+\gamma,\ 3\alpha+\gamma-\delta,\ -\alpha+3\beta+\gamma,\ 3\beta+\gamma-\delta,\ -\alpha+\gamma+3\delta,\ -\beta+\gamma+3\delta,$$
$$3\alpha-\beta+\delta,\ 3\alpha-\gamma+\delta,\ -\alpha+3\beta+\delta,\ 3\beta-\gamma+\delta,\ -\alpha+3\gamma+\delta,\ -\beta+3\gamma+\delta\}$$

R(x)=(x-vs[[1]])(x-vs[[2]])⋯(x-vs[[24]])を作ると,R(x)は$\alpha,\beta,\gamma,\delta$の対称式. 解と係数の関係により $\{\alpha, \beta, \gamma, \delta\}$ の 1,2,3,4次数対称式の値は{0,-10,-1,0}なので，R(x)は次の様な整数係数の多項式になる．(計算には10秒程度の時間がかかります.)

In[5]:=
```
Product[(x - vs[[k]]), {k, 1, Length[vs]}] //
 SymmetricReduction[#, {α, β, γ, δ}, {0, -10, 0, 1}] &
```

Out[5]=
$$\{2\,845\,177\,430\,298\,890\,625 - 2\,005\,037\,381\,967\,738\,300\,x^2 +$$
$$540\,254\,637\,222\,727\,266\,x^4 - 74\,964\,181\,748\,810\,700\,x^6 + 6\,115\,603\,032\,316\,015\,x^8 -$$
$$314\,736\,576\,091\,000\,x^{10} + 10\,611\,439\,620\,700\,x^{12} - 238\,205\,543\,800\,x^{14} +$$
$$3\,554\,349\,295\,x^{16} - 34\,525\,900\,x^{18} + 207\,970\,x^{20} - 700\,x^{22} + x^{24},\ 0\}$$

SymmetricReductionの出力は，第1成分が基本対称式による変形，第２成分がその残りなので，ここでは第２成分が0であることを確認し，第1成分をR(x)と定めて，因数分解する．

In[6]:=
```
Factor[%[[1]]]
```

Out[6]=
$$\left(3249 - 186\,x^2 + x^4\right)\left(529 - 154\,x^2 + x^4\right)\left(5329 - 154\,x^2 + x^4\right)$$
$$\left(2209 - 106\,x^2 + x^4\right)\left(625 - 58\,x^2 + x^4\right)\left(225 - 42\,x^2 + x^4\right)$$

vsの第 1 項をvとおく．即ちv=$\alpha + 3\,\beta - \gamma$．これが原始元となる．また $\alpha, \beta, \gamma, \delta$の取り方の順序は任意なので，vの満たす方程式V[x]（Galois 分解方程式) をR(x)の 6 番目のカッコ内の式に決めて良い．（6 番目のカッコの中の式が一番簡単そうなので)

In[7]:=
```
V[x_] = (List @@ %)[[6]]
```

Out[7]=
$$225 - 42\,x^2 + x^4$$

以上が解と係数の関係を利用した原始元と分解方程式の求め方となります .理論的には分かりやすいですが,次数が増えると計算時間が指数関数的に伸びていきます.

§1 - B. Grobener基底の利用(試行錯誤で見つけました)

fの基本対称式: s1,s2,s3,s4の値と v=$\alpha + 3\,\beta - \gamma$を素にしてGrobner基底を求める．その第1項が R(v)となる

In[8]:=
```
s1 = SymmetricPolynomial[1, {α, β, γ, δ}];(*α+β+γ+δ*)
s2 = SymmetricPolynomial[2, {α, β, γ, δ}];(*α β+α γ+β γ+α δ+β δ+γ δ*)
s3 = SymmetricPolynomial[3, {α, β, γ, δ}];(*α β γ+α β δ+α γ δ+β γ δ*)
s4 = SymmetricPolynomial[4, {α, β, γ, δ}];(*α β γ δ*)

GroebnerBasis[{s1, s2 + 10, s3, s4 - 1, v - (α + 3 β - γ)}, {δ, γ, β, α, v}][[1]]
Factor[%]
V[x_] = (List @@ %)[[6]] /. {v → x}
```

Out[12]=
$$2\,845\,177\,430\,298\,890\,625 - 2\,005\,037\,381\,967\,738\,300\,v^2 + 540\,254\,637\,222\,727\,266\,v^4 -$$
$$74\,964\,181\,748\,810\,700\,v^6 + 6\,115\,603\,032\,316\,015\,v^8 - 314\,736\,576\,091\,000\,v^{10} + 10\,611\,439\,620\,700\,v^{12} -$$
$$238\,205\,543\,800\,v^{14} + 3\,554\,349\,295\,v^{16} - 34\,525\,900\,v^{18} + 207\,970\,v^{20} - 700\,v^{22} + v^{24}$$

Out[13]=
$$\left(3249 - 186\,v^2 + v^4\right)\left(529 - 154\,v^2 + v^4\right)\left(5329 - 154\,v^2 + v^4\right)$$
$$\left(2209 - 106\,v^2 + v^4\right)\left(625 - 58\,v^2 + v^4\right)\left(225 - 42\,v^2 + v^4\right)$$

Out[14]=
$$225 - 42\,x^2 + x^4$$

先ほど求めた R(x)の式と同じ式が　遥かに短時間で求められます.

§2. α,β,γ,δを，原始元 v=α+3β-γ で表す

v = α + 3 β - γを原始元としてf (x) の解を全て v の多項式で表します .

2 - A. 解と係数の関係とユークリッドの互除法を使う(参考文献[7][8])

2- A-1. β,γ,δの対称式をαの式で表す.(f[x]を(x-α)で割った商は (x-β)(x-γ)(x-δ)であることを使う)

In[15]:=
```
PolynomialQuotient[f[x], x - α, x]
CoefficientList[%, x] // Reverse
```

Out[15]=

$$x^3 - 10\,\alpha + x^2\,\alpha + \alpha^3 + x\,\left(-10 + \alpha^2\right)$$

Out[16]=

$$\left\{1,\ \alpha,\ -10 + \alpha^2,\ -10\,\alpha + \alpha^3\right\}$$

f（x）=（x − α）（x − β）（x − γ）（x − δ）だから
β + γ + δ = −α, βγ + βδ + γδ = −10 + α², β γ δ = − (−10 α + α³) −−（#1）
(上の関係は解と係数の関係からも求まる)

2- A-2. vを原始元としてαを vで表す

In[17]:=
```
vs
```

Out[17]=

$$\{\alpha + 3\,\beta - \gamma,\ \alpha + 3\,\beta - \delta,\ \alpha - \beta + 3\,\gamma,\ \alpha + 3\,\gamma - \delta,\ \alpha - \beta + 3\,\delta,\ \alpha - \gamma + 3\,\delta,$$
$$3\,\alpha + \beta - \gamma,\ 3\,\alpha + \beta - \delta,\ -\alpha + \beta + 3\,\gamma,\ \beta + 3\,\gamma - \delta,\ -\alpha + \beta + 3\,\delta,\ \beta - \gamma + 3\,\delta,$$
$$3\,\alpha - \beta + \gamma,\ 3\,\alpha + \gamma - \delta,\ -\alpha + 3\,\beta + \gamma,\ 3\,\beta + \gamma - \delta,\ -\alpha + \gamma + 3\,\delta,\ -\beta + \gamma + 3\,\delta,$$
$$3\,\alpha - \beta + \delta,\ 3\,\alpha - \gamma + \delta,\ -\alpha + 3\,\beta + \delta,\ 3\,\beta - \gamma + \delta,\ -\alpha + 3\,\gamma + \delta,\ -\beta + 3\,\gamma + \delta\}$$

vsのうち αの係数がvと同じとなるものを見つけ(この場合は最初の6個)，その全ての積を取る．すると β, γ, δの対称式ができる．これを(#1)を使って変形する.

In[18]:=
```
g1[x_] = Product[(x - vs[[i]]), {i, 1, 6}]
g1[x_] = SymmetricReduction[%, {β, γ, δ}, {-α, -10 + α^2, -(-10 α + α^3)}][[1]] //
  Collect[#, {x, α}] &
```

Out[18]=

$$(x - \alpha + \beta - 3\,\gamma)\,(x - \alpha - 3\,\beta + \gamma)\,(x - \alpha + \beta - 3\,\delta)\,(x - \alpha + \gamma - 3\,\delta)\,(x - \alpha - 3\,\beta + \delta)\,(x - \alpha - 3\,\gamma + \delta)$$

Out[19]=

$$-144\,000 + x^6 - 2\,x^5\,\alpha + 108\,100\,\alpha^2 - 20\,260\,\alpha^4 + 1105\,\alpha^6 + x^4\,\left(-260 + 19\,\alpha^2\right) +$$
$$x^3\,\left(-120\,\alpha + 28\,\alpha^3\right) + x^2\,\left(16\,900 - 1960\,\alpha^2 + 35\,\alpha^4\right) + x\,\left(49\,400\,\alpha - 9400\,\alpha^3 + 414\,\alpha^5\right)$$

「v=vs[[1]]=α + 3 β - γ 」なので g1[v] = 0 が成り立つ．　g1[x]のαをyに変えg1[x,y]を作り，さらに xをvと名前を変えg1v[y]を作る．このとき v の式を V(x)で割った余りを考え，簡単にしておく.

In[20]:=
```
g1[x_, y_] = g1[x] /. {α → y}
g1v[y_] = g1[v, y] // PolynomialMod[#, V[v]] & // Collect[#, y] &
```

Out[20]=
$$-144\,000 + x^6 - 2\,x^5\,y + 108\,100\,y^2 - 20\,260\,y^4 + 1105\,y^6 + x^4\left(-260 + 19\,y^2\right) + x^3\left(-120\,y + 28\,y^3\right) + x^2\left(16\,900 - 1960\,y^2 + 35\,y^4\right) + x\left(49\,400\,y - 9400\,y^3 + 414\,y^5\right)$$

Out[21]=
$$-94\,950 + 7519\,v^2 + \left(49\,850\,v - 204\,v^3\right)y + \left(103\,825 - 1162\,v^2\right)y^2 + \left(-9400\,v + 28\,v^3\right)y^3 + \left(-20\,260 + 35\,v^2\right)y^4 + 414\,v\,y^5 + 1105\,y^6$$

g1v（α）= g1（v, α）= g1（v）= 0 だから，f（y）とg1v（y）はy = αを共通解に持つ.
さらにg1v（β）≠ 0, g1v（γ）≠ 0, g1v（δ）≠ 0 から　共通解はy＝αのみである.
故に，ユークリッドの互除法を使いf（y）とg1v（y）の最大公約式を求めると
それは（y − α）となる．これでαはvの式で表される.
ユークリッドの互除法を実現するために，PolynomialRemainder
で余りを繰り返し求める.まずはg1v[y] をf[y] で割った余り r1[y] を求める.

In[22]:=
```
r1[y_] =
 PolynomialRemainder[g1v[y], f[y], y] // PolynomialMod[#, V[v]] & // Collect[#, y] &
```

Out[22]=
$$-85\,740 + 7484\,v^2 + \left(49\,436\,v - 204\,v^3\right)y + \left(10\,620 - 812\,v^2\right)y^2 + \left(-5260\,v + 28\,v^3\right)y^3$$

次にf[y]をr1[y] で割った余り r2[y] を求める.

In[23]:=
```
r2[y_] =
 PolynomialRemainder[f[y], r1[y], y] // PolynomialMod[#, V[v]] & // Collect[#, y] &
```

Out[23]=
$$\frac{32\,227\,200 - 5\,601\,920\,v^2}{3\,679\,200 + 1\,031\,416\,v^2} + \frac{\left(5\,243\,520\,v - 149\,120\,v^3\right)y}{3\,679\,200 + 1\,031\,416\,v^2} + \frac{\left(-7\,833\,600 + 689\,920\,v^2\right)y^2}{3\,679\,200 + 1\,031\,416\,v^2}$$

次にr1[y] をr2[y] で割った余り r3[y] を求める.

In[24]:=
```
r3[y_] =
 PolynomialRemainder[r1[y], r2[y], y] // PolynomialMod[#, V[v]] & // Collect[#, y] &
```

Out[24]=
$$\frac{264\,554\,019\,000 - 51\,898\,817\,880\,v^2}{-27\,912\,825 + 5\,604\,522\,v^2} + \frac{\left(113\,338\,683\,000\,v - 5\,541\,649\,560\,v^3\right)y}{-27\,912\,825 + 5\,604\,522\,v^2}$$

これはyの一次式なのでこれを yについて解くと, αはvの式で表される (これを α0とおく)

In[25]:=
```
α0 = y /. Solve[r3[y] == 0, y][[1]]
```

Out[25]=
$$\frac{244\,957\,425 - 48\,054\,461\,v^2}{v\left(-104\,943\,225 + 5\,131\,157\,v^2\right)}$$

これがαをvで表した有理式．このままでは計算が大変なので，V（v）を分母の因子（ここでは2個）
で割る事により整式に直し，改めてα' と名付ける.

In[26]:=
```
bunbo1 = (List @@ Denominator[α0])[[1]](*Denominatorは分母*)
bunbo2 = Plus @@ (List @@ Denominator[α0])[[2]]
```

Out[26]=
```
v
```

Out[27]=
$$-104\,943\,225 + 5\,131\,157\,v^2$$

In[28]:=
```
{q1, r1} = PolynomialQuotientRemainder[V[v], bunbo1, v];
(*V(v)をbunbo1で割った商がq1,余りがr1*)
{q2, r2} = PolynomialQuotientRemainder[V[v], bunbo2, v];
α' = (-q1 / r1) * (-q2 / r2) * (Numerator[α0]) // PolynomialMod[#, V[v]] & //
  Expand(*Numeratorは分子*)
```

Out[30]=
$$\frac{4\,v}{15} - \frac{v^3}{45}$$

これが α を vの整式で表した式となる．同様にして，β，γ，
δもvの式で表すことができるが，次の Grobner基底を使う方が速いのでここでは省略する．

---

2 - B. Grobener基底の利用(試行錯誤で見つけました)

先ずは αをvで表す．V[x] をGrobener基底を使って求めた時と殆ど同じだが，αとvを残すように指定する．

In[31]:=
```
GroebnerBasis[{s1, s2 + 10, s3, s4 - 1, v - (α + 3 β - γ)}, {α, v}, {δ, γ, β}] //
  PolynomialMod[Last[#], V[v]] &;
α' = α /. Solve[% == 0, α][[1]] // Collect[#, v] &
```

Out[32]=
$$\frac{4\,v}{15} - \frac{v^3}{45}$$

先の結果と一致した．同様に，β, γ, δをvの式で表すことができる．最後に $\{\alpha,\beta,\gamma,\delta\}$をまとめて表示する．

In[33]:=
```
GroebnerBasis[{s1, s2 + 10, s3, s4 - 1, v - (α + 3 β - γ)}, {β, v}, {δ, γ, α}] //
  PolynomialMod[Last[#], V[v]] &;
β' = β /. Solve[% == 0, β][[1]] // Collect[#, v] &;
GroebnerBasis[{s1, s2 + 10, s3, s4 - 1, v - (α + 3 β - γ)}, {γ, v}, {δ, β, α}] //
  PolynomialMod[Last[#], V[v]] &;
γ' = γ /. Solve[% == 0, γ][[1]] // Collect[#, v] &;
GroebnerBasis[{s1, s2 + 10, s3, s4 - 1, v - (α + 3 β - γ)}, {δ, v}, {γ, β, α}] //
  PolynomialMod[Last[#], V[v]] &;
δ' = δ /. Solve[% == 0, δ][[1]] // Collect[#, v] &;
sols = {α', β', γ', δ'}
```

Out[39]=
$$\left\{\frac{4\,v}{15} - \frac{v^3}{45},\ -\frac{4\,v}{15} + \frac{v^3}{45},\ -\frac{23\,v}{15} + \frac{2\,v^3}{45},\ \frac{23\,v}{15} - \frac{2\,v^3}{45}\right\}$$

§3. vs1,vs2,...,vs24のうちV[x]の解となるものを見つけ，それをvで表す

vsの要素は24個あるが，このうちV (x) の解となっているものを見つける． やり方は
[1] {α,β, γ, δ}をvで表した式を使い vs の要素を全てvで表す．
[2] これをV[x]に代入して0となる vs の要素を見つける
という力技である．

In[40]:=
```
vs /. {α → α', β → β', γ → γ', δ → δ'} // Simplify;(*vsの要素をvで表す*)
PolynomialMod[V[#], V[v]] & /@ %;
Position[%, 0] // Flatten
vs[[%]]
vset = % /. {α → α', β → β', γ → γ', δ → δ'} // Collect[#, v] &
```

Out[42]=
$$\{1, 8, 17, 24\}$$

Out[43]=
$$\{\alpha + 3\,\beta - \gamma,\ 3\,\alpha + \beta - \delta,\ -\alpha + \gamma + 3\,\delta,\ -\beta + 3\,\gamma + \delta\}$$

Out[44]=
$$\left\{v,\ -v,\ \frac{14\,v}{5} - \frac{v^3}{15},\ -\frac{14\,v}{5} + \frac{v^3}{15}\right\}$$

上の vset = vs[[{1,8,17,24}]]={α + 3 β - γ, 3 α + β - δ, -α + γ + 3 δ, -β + 3 γ + δ}=$\left\{v,\ -v,\ \frac{14\,v}{5} - \frac{v^3}{15},\ -\frac{14\,v}{5} + \frac{v^3}{15}\right\}$ が V[x] の解となる．

§4. f[x]の解のガロア群を求める

vset={v1,v2,v3,v4}とする． α, β ,γ,δは原始元v (=v1) の式で表されているので v1をv1,v2, v3,v4にそれぞれ変えると vsetが変化する． 例えば v1→v2とすると
vset→{-v,v,$-\frac{14\,v}{5} + \frac{v^3}{15}, \frac{14\,v}{5} - \frac{v^3}{15}$}={v2,v1,v4,v3}と変わる． この例では V(x)の解:vset の置換群は
G_V={{v1,v2,v3,v4},{v1,v2,v3,v4},{v1,v2,v3,v4},{v1,v2,v3,v4}}となる．

一方，この置換を f(x)の解の置換と見ることもできる． α, β ,γ,δは全てvの式で表されているので， v1→v2のとき， α, β ,γ,δは次のように変化する．
{α, β ,γ,δ}=$\left\{\frac{4\,v}{15} - \frac{v^3}{45},\ -\frac{4\,v}{15} + \frac{v^3}{45},\ -\frac{23\,v}{15} + \frac{2\,v^3}{45},\ \frac{23\,v}{15} - \frac{2\,v^3}{45}\right\}$→
$\left\{-\frac{4\,v}{15} + \frac{v^3}{45},\ \frac{4\,v}{15} - \frac{v^3}{45},\ \frac{23\,v}{15} - \frac{2\,v^3}{45},\ -\frac{23\,v}{15} + \frac{2\,v^3}{45}\right\}$={ β ,α,δ,γ}
{α, δ,β, γ}⇔{1,2,3,4} と対応させると(1,2,3,4)→(2,1,4,3) という置換になる.これを「 v1→v1,v1→v2,v1→v3,v1→v4 」の各々 について実行すると， f(x)の解についての置換(GaloisによるGalois群)が得られる．

以上から分かるように Galois群の位数は V(x)の次数と一致する． $f(x) = x^4 - 10\,x^2 + 1$ のときは「たまたま」V(x)の次数が f(x)の次数と一致しているが， 4個の解の置換は最大4!=24通りあり， Galois群の位数=V(x)の次数=24 となり得る． 今回は簡単のためにできるだけ位数の小さくなるケースを選んだので， 一致してしまったが， 通常は一致しない． 例えば§5の例「 $f(x) = x^4 - 2$ 」を参照して頂きたい． 以上を, Mathematicaでは 次の様にして実行出来る．

In[45]:=
```
sols = {α', β', γ', δ'};
Table[
  perm = sols /. {vset[[1]] → vset[[i]]} // PolynomialMod[#, V[v]] &;
  Table[FirstPosition[Simplify[perm - sols[[k]] {1, 1, 1, 1}], 0][[1]], {k, 1, 4}] //
   Flatten, {i, 1, Length[vset]}];
MatrixForm[%]
```

Out[47]//MatrixForm=

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

これがGalois群のガロアによる表現． f(x)の解の入れ替えは一行目からスタートすると
{1,2,3,4}→{1,2,3,4},{1,2,3,4}→{4,3,2,1},{1,2,3,4}→{3,4,1,2},{1,2,3,4}→{2,1,4,3}
を表すが，これを2行目からスタートして
{4,3,2,1}→{1,2,3,4},{4,3,2,1}→{4,3,2,1},{4,3,2,1}→{3,4,1,2},{4,3,2,1}→{2,1,4,3}
と読んでも良い．3行目/4行目からスタートしても同じになる(参考文献[6])

現代の表現では次の様になり，Galois群は「クラインの4元群」となることが分かる(Idは単位元)
{ Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)}

{v1,v2,v3,v4}の置換群も同様に（より簡単に) 得ることができるが省略する.

§5. [参考] SageMath & Magma &まとめ

5-1. SageMath&Magma

フリーの SageMath や Magma calculator を使うと，ガロア群はすぐ求まる．例えば SageMath では次の様になる．

```
_. < x > = PolynomialRing (QQ)
f = x^4-10*x^2 + 1
G = f . galois_group ()
G . list ()
```

Magma calculator では次の様になる. 結果は生成元で表される.

```
_<x>:=PolynomialAlgebra(Rationals());
//PolynomialRing も大丈夫
f:=x^4-10*x^2 + 1;
G:=GaloisGroup(f); G;
```

SageMath は完全無料で Windows/Macにインストールもできる．ただ 最新版(ver.10)のインストールはやや面倒そうなので，私はWindows にver9 を入れています．
これらは作成したファイルも保存できるので私には Magmaより使いやすい. なお Linuxではほとんどの distribu-tionに最初から入っているそうです．
さらに インストールなしにwebから使える SageMathCell，Android/iOS で使える SageCalculator もあります．なお，SageMathではvsetの置換群も求めることができます．

Magma は有料で,そのうえ研究機関にしか販売していないのでインストールは敷居が高いですが，Web上で calculator として無料で使えます．
残念ながらcalculator ではファイルの保存はできません．(コピペしてtext file で保存する事はできます)

MagmaやSageMathを使って Galois群をご覧になりたい方は，**`https://mixedmoss.com/mathematica/Galois/`** により詳しい説明が置いてあります．

5-2. StepByStep Mathematica Program (R(x)のチェックが必要)

残念ながら私の知る限り Mathematica ではMagmaやSageMathのようなコマンドはありません . しかし5次ぐらいまでなら, 今までと同様にして求めることができます.
以下は4次方程式に対するプログラムです . §1~4の内容を完結にまとめたものです. ここでR (x) が重解を持つときはvsのリストの変更が必要です . そのためにR (x) を出力させてます . (しかしそういうケースは非常に稀です .)

Step1 . 分解方程式

出力は 24次の方程式R (x), そして分解方程式V(x)です. 例として (x^4 - 2) のGalois群を求めます.

```
ClearAll["`*"]
f[x_] = x^4 - 2;
vars = {α, β, γ, δ};
vs = Permutations[vars].{1, 3, -1, 0}; (*R(x)に重解があるときはここを変える*)
coef = CoefficientList[f[x], x] // Reverse // Drop[#, 1] &;
{s1, s2, s3, s4} = Table[SymmetricPolynomial[i, vars], {i, 1, 4}];
contents = {s1 + coef[[1]], s2 - coef[[2]], s3 + coef[[3]], s4 - coef[[4]], v - vs[[1]]};
r = GroebnerBasis[contents, {δ, γ, β, α, v}][[1]] // Factor (*重解を持たないことの確認はここで*)
V[v_] = If[IrreduciblePolynomialQ[r], r, Last@(List @@ Factor[r])]
```

Out[108]=

$$\left(334\,084 - 644\,v^4 + v^8\right)\left(2500 + 28\,v^4 + v^8\right)\left(114\,244 + 476\,v^4 + v^8\right)$$

Out[109]=

$$114\,244 + 476\,v^4 + v^8$$

Step2 . f (x)の解を原始元vで表す

In[57]:=

```
GroebnerBasis[contents, {α, v}, {δ, γ, β}] // PolynomialMod[Last[#], V[v]] &;
α' = α /. Solve[% == 0, α][[1]] // Collect[#, v] &;
GroebnerBasis[contents, {β, v}, {δ, γ, α}] // PolynomialMod[Last[#], V[v]] &;
β' = β /. Solve[% == 0, β][[1]] // Collect[#, v] &;
GroebnerBasis[contents, {γ, v}, {δ, β, α}] // PolynomialMod[Last[#], V[v]] &;
γ' = γ /. Solve[% == 0, γ][[1]] // Collect[#, v] &;
GroebnerBasis[contents, {δ, v}, {γ, β, α}] // PolynomialMod[Last[#], V[v]] &;
δ' = δ /. Solve[% == 0, δ][[1]] // Collect[#, v] &;
sols = {α', β', γ', δ'}
```

Out[65]=

$$\left\{\frac{199\,v}{520} + \frac{v^5}{1040},\ \frac{61\,v}{780} - \frac{v^5}{1560},\ -\frac{199\,v}{520} - \frac{v^5}{1040},\ -\frac{61\,v}{780} + \frac{v^5}{1560}\right\}$$

Step 3 . V(x)の解を原始元vで表す

In[66]:=
```
vs /. {α → α', β → β', γ → γ', δ → δ'} // Simplify;
PolynomialMod[V[#], V[v]] & /@ %;
Position[%, 0] // Flatten;
vset = vs[[%]] /. {α → α', β → β', γ → γ', δ → δ'} // Collect[#, v] &
```

Out[69]=

$$\left\{v, \frac{69\,v}{130}+\frac{v^5}{260}, \frac{407\,v}{312}+\frac{v^5}{624}, -\frac{119\,v}{120}-\frac{v^5}{240}, -\frac{69\,v}{130}-\frac{v^5}{260}, -v, \frac{119\,v}{120}+\frac{v^5}{240}, -\frac{407\,v}{312}-\frac{v^5}{624}\right\}$$

Step4 . Galois群を求める

In[70]:=
```
Table[
  perm = sols /. {vset[[1]] → vset[[i]]} // PolynomialMod[#, V[v]] &;
  Table[FirstPosition[Simplify[perm - sols[[k]] {1, 1, 1, 1}], 0][[1]], {k, 1, 4}] //
   Flatten, {i, 1, Length[vset]}];
MatrixForm[Sort[%]]
```

Out[71]//MatrixForm=

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \\ 2 & 1 & 4 & 3 \\ 2 & 3 & 4 & 1 \\ 3 & 2 & 1 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

今度はGalois群の位数は8となりました．V(x)も8次です．

5-3. Automated Mathematica Program (次数は実用上5次まで．重解チェックは不要)

次のプログラムでは「一応5次まで」の方程式のGalois群が求まるプログラムです．理論的には6次,7次でも可能なはずですが，メモリーや時間の制限があり，実際は5次方程式が限界な気がします．またR(x)に重解がでてきた場合，それを自動でチェックし他の係数を選ぶように作ってあります．かつ説明文を無くし１つのセルにまとめてあります．従って「**最初のｆさえ入力して下のセルを評価（Shift+Enter）**」すれば，自動で（5次くらいまでなら) Galois群を求めることが出来ます．

出力は Galois群だけですが，全て Global 変数のままなので 評価後に変数の値を見ることが可能です．例えば「分解方程式」→ V[x],「f(x)の解の 原始元vによる表現」→sols（リスト)，「V[x]=0の解の vによる表現」→vset (リスト)，「vsに使われた係数」→selected　と入力すると，中身を見ることが出来ます．

Module化して関数にすることも考えましたが，非常に読みづらくなるのでやめました．（関数の中では%が使えないので変数が増える．V[x]をModule内で定義できないので「/.」による代入に変えないといけない．さらにもっと良いアルゴリズムがあるはずなど．）　なお，実行時間を「Timing」で測ろうとしたのですが，なぜかうまく行きませんでした．残念です．

既約であっても大丈夫ですが，$\left(x^4+2x^2+1\right)$など，重解を持つときは駄目です．Magma はこのような時も答えを出してきますが，その場合は重解の間の入れ替えは考えないようです．SageMathは既約の場合は全く答えが出ません．

下の例は5次方程式で Galois群が D_5のものです．私のPCで30秒でしたが，Galois群が F_{20}の場合はもっと時間がかかり，2分ぐらいかかりました．Magma や SageMath の 0.1秒未満とは比較になりません．まったくアルゴリズムが違うのでしょう．これがModule化しない大きな理由の1つです．

In[72]:=
```
(*下のf[x] を変えて「このセルを評価」
  するだけです.ただし重解を持ってはいけません.また5次までがオススメです. *)
Clear["`*"]
f[x_] = x^5 - 5 x + 12;

(*[Step0]重解を持たないようなvsの係数を見つけて selected に入れる.*)
n = Exponent[f[x], x];
sols = x /. NSolve[f[x] == 0, x];
allsets = Subsets[Range[-5, 5], {n}];
selected = RandomChoice[allsets];
While[Min@Abs@Differences@Sort@(Permutations[selected].sols) < 0.01,
  selected = RandomChoice[allsets]];

(*[Step1]分解方程式V(x)を求める.ここは先のプログラムとほぼ同じです*)
vars = Take[{x1, x2, x3, x4, x5, x6, x7, x8, x9, x10}, n];
(*ここを変えると, 理論的には何次でも大丈夫なはず*)
vs = Permutations[vars].selected;
coef = CoefficientList[f[x], x] // Reverse // Drop[#, 1] &;
syms = Table[SymmetricPolynomial[i, vars], {i, 1, n}];
contents = Append[syms + coef * Table[(-1)^(k - 1), {k, 1, n}], v - vs[[1]]];
rs = GroebnerBasis[contents, Append[vars, v]][[1]];
V[v_] = If[IrreduciblePolynomialQ[rs], rs, Last@(List @@ Factor[rs])];

(*[Step2]原始元vを使ってf(x)の解を表す. 先のプログラムをTableでまとめているだけです. *)
sols = Table[base = GroebnerBasis[contents, {vars[[i]], v}, Drop[vars, {i}]] //
      PolynomialMod[Last[#], V[v]] &;
   vars[[i]] /. Solve[base == 0, vars[[i]]][[1]] // Collect[#, v] &, {i, 1, n}];

(*[Step3]V(x)の解の集合vsを,その第1要素v(=v1)の式で表す.
先のプログラムとほぼ同じですが, Galois群がSnの時はバイパスしています*)
If[! IrreduciblePolynomialQ[rs], vs' = vs /. AssociationThread[vars → sols] // Simplify;
  values = PolynomialMod[V[#], V[v]] & /@ (vs');
  pos = Position[values, 0] // Flatten;
  vset = vs'[[pos]] // Collect[#, v] &];

(*[Step4]Galois群を求める.
 これも先のプログラムと全ど同じですが, Galois群がSnの時はバイパスしています*)
If[! IrreduciblePolynomialQ[rs],
  Table[
   perm = sols /. {vset[[1]] → vset[[i]]} // PolynomialMod[#, V[v]] &;
   Table[FirstPosition[Simplify[perm - sols[[k]] × Table[1, n]], 0][[1]], {k, 1, n}] //
    Flatten, {i, 1, Length[vset]}],
  Permutations[Range[n]]];
MatrixForm[Sort[%]]
```

Out[89]//MatrixForm=

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \\ 2 & 1 & 4 & 3 & 5 \\ 2 & 4 & 1 & 5 & 3 \\ 3 & 1 & 5 & 2 & 4 \\ 3 & 5 & 1 & 4 & 2 \\ 4 & 2 & 5 & 1 & 3 \\ 4 & 5 & 2 & 3 & 1 \\ 5 & 3 & 4 & 1 & 2 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

In[90]:= `V[x]`

Out[90]=

$$12\,269\,860\,000 - 1\,395\,020\,000\,x + 362\,187\,500\,x^2 - 42\,295\,000\,x^3 + 6\,895\,000\,x^4 - 376\,300\,x^5 + 78\,925\,x^6 - 1100\,x^7 + 450\,x^8 + x^{10}$$

In[91]:= `sols[[1]]`

Out[91]=

$$\frac{71\,089\,493\,276\,166\,411\,761}{22\,129\,539\,137\,874\,030\,645} - \frac{4\,966\,597\,666\,488\,864\,623\,v}{7\,376\,513\,045\,958\,010\,215} + \frac{8\,536\,395\,927\,902\,214\,553\,v^2}{88\,518\,156\,551\,496\,122\,580} - \frac{77\,241\,731\,335\,993\,101\,v^3}{8\,196\,125\,606\,620\,011\,350} + \frac{348\,507\,725\,429\,357\,087\,v^4}{221\,295\,391\,378\,740\,306\,450} - \frac{177\,361\,226\,909\,144\,663\,v^5}{4\,425\,907\,827\,574\,806\,129\,000} + \frac{33\,675\,175\,668\,000\,691\,v^6}{2\,950\,605\,218\,383\,204\,086\,000} + \frac{389\,993\,753\,714\,573\,v^7}{8\,851\,815\,655\,149\,612\,258\,000} + \frac{1\,414\,453\,103\,375\,621\,v^8}{44\,259\,078\,275\,748\,061\,290\,000} + \frac{2\,979\,000\,924\,539\,v^9}{8\,851\,815\,655\,149\,612\,258\,000}$$

【参考文献&サイト】次のサイトや文献を参考にさせて頂きました．ありがとうございます．

1．可解な5次方程式について（大迎　規宏氏）□
2．方程式のガロア群（松田修氏）□
3．ガロア理論を使って方程式を解いたことがありますか（scruta氏）□
4．ペンギンは空を飛ぶ－ 5次方程式の解を巡る旅 （peng225氏）□
5．Period－Mathmatics 可解な5次方程式の代数的解法 □
（以下は書籍）□
6．ガロアの群論（中村亨氏）□
7．ガロワ理論最短コース（梶原　健氏）□
8．ガロア理論の頂きを踏む（石井俊全氏）□
9．ガロア理論「超」入門（小林吹代氏）□

全てのサイト&文献は，私を色々な意味で啓発してくれましたが，ガロア群を求めるときに特に参考にしたのは[7]と[8]です．５次方程式の解を求めるときは特に[1]と[6]と[7]を参考にしました．なお私は専門家ではないので，色々間違いしているかもしれません．その際はお知らせ下さると有り難いです．なおメールアドレスは　ロボット対策のため 画像となっています．クリックしても何も起こりません．(mail@mixedmoss.com)