合成多項式たちの終結式の鎖律における計算効率と幾何学的意味

早稲田大学大学院　基幹理工学研究科　数学応用数理専攻　修士 2 年

5111A009-4　猪野夏美

はじめに

終結式というと、1 変数 2 多項式が解を持つかどうかを判別する、多項式の係数を成分とする行列式、という定義が一般に広く知られている。
（厳密に定義すると、以下のようになる。$f, g \in k[x]$（k は体とする）を
$f := a_0x^m + a_1x^{m-1} + ... + a_m$、$g := b_0x^n + b_1x_{n-1} + ... + b_n$（$m, n > 0$）とおくとき、

$$f \text{ と } g \text{ の終結式 } (\mathrm{Res}(f,g) \text{ と表記}) := \begin{vmatrix} a_0 & ... & 0 & b_0 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ a_m & ... & 0 & b_n & ... & 0 \\ 0 & ... & a_0 & 0 & ... & b_0 \\ ... & ... & ... & ... & ... & ... \\ 0 & ... & a_m & 0 & ... & b_m \end{vmatrix}$$

（行 $a_0...a_m$ は n 列、行 $b_0...b_n$ は m 列並ぶので、上の行列式は大きさが $m+n$ の行列式となる）と定義される。）
この定義は 2 変数 2 斉次 多項式の場合にも拡張される（このときの終結式は斉次多項式たちが 非自明 解（$= \mathbf{P}^1(k)$ 内での解）をもつかどうかを判別する、斉次多項式たちの係数を成分とする行列式と定義される）。さらに n 変数 n 多項式の場合にも、それらの終結式は、n 変数 n 多項式が $\mathbf{P}^{n-1}(k)$ に解をもつかどうかを判別する行列式、と定義が一般化されている。
本論文では、その一般化された n 変数 n 多項式たちの終結式を扱う。
斉次多項式を斉次多項式に代入した合成斉次多項式たちの終結式の鎖律についてまとめられている論文 [4] を読んだ。[4] の主定理では、代入する斉次多項式たちの次数が全て同一の場合の鎖律についてまとめられていたが、その代入する斉次多項式たちの次数が「全て同一」でなくても同じように鎖律が成り立つのだろうかと疑問に思ったことが本論文作成のきっかけである。
その疑問は [1] を読むことで解決し、[4] の主定理において、代入する斉次多項式の次数が「全て同一」でなくても同じように鎖律が成り立つ、ということが分かった。
したがって、本論文で扱う定理は新しいものではないが、その既存の定理に対して、新しく、初等的に分かりやすく証明しなおしてみるというのが本論文の目的の一つである。
次に、その定理を使うことで終結式の計算を格段にしやすくなるのだが、定理を使う場合と使わない場合でどれくらい計算の早さ、計算量に違いが出てくるのかを見てみる。
そして、多項式たちの終結式が 0 になるということは $\mathbf{P}^{n-1}(\overline{k})$ 内に解をもつことを意味するが、言い変えるとそれらの多項式 $= 0$ としてグラフを描いたときに、原点以外の共有点をもつことになる。定理を使うことで複雑な図形たちが共通零点をもつことが分かる例を紹介する。
最後に、完全に多項式たちに多項式を代入した合成多項式たちの終結式だけでなく、部分的に多項式たちに多項式を代入した合成多項式の場合にも同じように鎖律のようなものが成り立つことが論文 [2] の主定理により分かるが、本論文ではその主定理の一般化を行う。

論文 [1] の主定理の証明

まず、扱う定理 (合成多項式たちの終結式の鎖律) を以下で紹介する。

定理 1

（[1] から引用）$\mathrm{Res}_{d_1m,d_2m,...,d_nm}(F_1(h_1,h_2,...,h_n)^h,F_2(h_1,h_2,...,h_n)^h,...,F_n(h_1,h_2,...,h_n)^h)$
$=(\mathrm{Res}_{d_1,d_2,...,d_n}(F_1,F_2,...,F_n))^{m^{n-1}}\times(\mathrm{Res}_{m,m,...,m}(x_n^{m-m_1}H_1,H_2,...,H_n))^{d_1d_2...d_n}$
$=(\mathrm{Res}_{d_1,d_2,...,d_n}(F_1,F_2,...,F_n)^{m^{n-1}}\times(\mathrm{Res}_{m_1,m,...,m}(H_1,H_2,...,H_n))^{d_1d_2...d_n}\times(\mathrm{Res}_{m,...,m}(\overline{H_2},...,\overline{H_n}))^{(m-m_1)d_1d_2...d_n}$

ここで F_1,F_2,...,F_n は次数 d_1,d_2,...,d_n の体 k 係数 n 変数斉次多項式、H_1,H_2,...,H_n は次数 m_1,m,...,m の体 k 係数 n 変数斉次多項式 $(m_1<m)$ とし、
$h_i:=H_i(x_1,x_2,...,x_{n-1},1)$,$\overline{H_i}:=H_i(x_1,x_2,...,x_{n-1},0)$,$F_i(h_1,h_2,...,h_n)^h$は $F_i(h_1,h_2,...,h_n)$ を斉次化させた多項式とする。$(i=1,2,...,n)$

定理 1 を証明するために必要な諸定理を以下で紹介する。

まず、終結式の定義も伴う次の定理 2 を紹介する。

定理 2

（[3] から引用）次数 d_1,d_2,...,d_n の体 k 係数 n 変数斉次多項式 F_1,F_2,...,F_n に対して、
$F_1,F_2,...,F_n$ の係数たちを変数とする $\mathbf{Z}$ 係数多項式 $\mathrm{Res}_{d_1,d_2,...,d_n}(F_1,F_2,...,F_n)$ が存在して $\mathrm{Res}_{d_1,d_2,...,d_n}(F_1,F_2,...,F_n)=0$
$\Longleftrightarrow F_1=F_2=...=F_n=0$ は $\mathbf{P}^{n-1}(\overline{k})$ に解を持つ。
が成り立つ。このときの $\mathrm{Res}_{d_1,d_2,...,d_n}(F_1,F_2,...,F_n)$ を $F_1,F_2,...,F_n$ たちの終結式と呼ぶ。
ここで、$\overline{k}$ は k の代数的閉体とする。

次に、定理 1 を証明するときに重要な次の定理を紹介する。

定理 3

（[4] から引用）$\mathrm{Res}_{d_1m,d_2m,...,d_nm}(F_1(H_1,H_2,...,H_n),F_2(H_1,H_2,...,H_n),...,F_n(H_1,H_2,...,H_n))$
$=(\mathrm{Res}_{d_1,d_2,...,d_n}(F_1,F_2,...,F_n))^{m^{n-1}}\times(\mathrm{Res}_{m,m,...,m}(H_1,H_2,...,H_n))^{d_1d_2...d_n}$

定理 2 と定理 3 を使って、定理 1 を証明する。

定理 1 の証明

主定理を証明する前に、何故 H_1,H_2,...,H_n の次数を m_1,m,...,m（$m_1<m$）として終結式の鎖律を考えるのかを説明する。そのために H_1,H_2,...,H_n の次数を m_1,m,...,m ではなく、m_1,m_2,...,m_n と表記して考える。
m_1,m_2,...,m_n のうち、少なくとも 2 つの m_i と m_j（1≦ i < j≦ n）が $m:=max(m_1,m_2,...,m_n)$ よりも小さくなるとき、
$\mathrm{Res}(F_1(h_1,h_2,...,h_n)^h,F_2(h_1,h_2,...,h_n)^h,...,F_n(h_1,h_2,...,h_n)^h)$
が恒等的に 0 になる、すなわち、定理 1 の Resultant の chain rule は成り立たないことを証明する。
$(i,j)=(1,2)$ として一般性を失わないので、$(i,j)=(1,2),m_1=m_2<m_3=...=m_n=m$ として考える。
計算すると $F_i(h_1,h_2,.h_3,...,h_n)^h=F_i(x_n^{m-m_1}H_1,x_n^{m-m_1}H_2,H_3,...,H_n)$ となることがわかる。
3≦ k となる k に対して、$h_k=h_k^{(m)}+h_k^{(m-1)}+...+h_k^{(0)}$（$h_k^{(i)}$ は h_k の i 次斉次部分（$i=1,2,...,n$））と書く。
方程式系 $h_3^{(m)}=...=h_n^{(m)}$ は, 未知数 $n-1$ 個で、式数が $n-2$ 本の方程式系となるので、必ず $\mathbf{P}^{n-2}(\overline{k})$ に解を持つ。（その解を $(a_1,a_2,...,a_{n-1})$ とする。）
すると、$(a_1,a_2,...,a_{n-1},0)\in\mathbf{P}^{n-1}(\overline{k})$ は $x_n^{m-m_1}H_1=x_n^{m-m_1}H_2=H_3=...=H_n=0$ の解となる。F_i は斉次多項式であるので、$F_i(0,0,...,0,0)=0(i=1,2,...,n)$ が成り立つ。したがって、$(a_1,a_2,...,a_{n-1},0)\in\mathbf{P}^{n-1}(\overline{k})$ は $F_1(h_1,h_2,...,h_n)^h=F_2(h_1,h_2,...,h_n)^h=...=F_n(h_1,h_2,...,h_n)^h=0$ の解となる。

よって、定理 2 より、
$\mathrm{Res}_{d_1m_1,d_2m_2,d_3m,...,d_nm}(F_1(h_1,h_2,...,h_n)^h,F_2(h_1,h_2,...,h_n)^h,...,F_n(h_1,h_2,...$
$,h_n)^h)=0$
が成り立つ。
したがって、$(m_1,m_2,...,m_n)=(m_1,m,...,m)$ ($m_1<m$) として考えないと、終結式の鎖律が成り立たないので、
H_1,H_2,...,H_n の次数を m_1,m,...,m（$m_1<m$）として考える。
定理 3 を使って、定理 1 の前半を証明する。
定理 3 を使うと、
$\mathrm{Res}_{d_1m,d_2m,...,d_nm}(F_1(h_1,h_2,...,h_n)^h,F_2(h_1,h_2,...,h_n)^h,...,F_n(h_1,h_2,...,h_n)^h)$
$=\mathrm{Res}_{d_1m,d_2m,...,d_nm}(F_1(x_n^{m-m_1}H_1,H_2,...,H_n),F_2(x_n^{m-m_1}H_1,H_2,...,H_n),...$
$,F_n(x_n^{m-m_1}H_1,H_2,...,H_n))=$
$(\mathrm{Res}_{d_1,d_2,...,d_n}(F_1,F_2,...,F_n))^{m^{n-1}}\times(\mathrm{Res}_{m,m,...,m}(x_n^{m-m_1}H_1,H_2,...,H_n))^{d_1d_2...d_n}$
が成り立ち、定理 1 の前半が示された。

定理 1 の後半を示すために、次の定理を用いる。

定理 4

（[5] から引用）$\mathrm{Res}_{d_1,d_2,...,d_n}(F_1,F_2,...,F_n)$
$=(\mathrm{Res}_{d_1,d_2,...,d_{n-1}}(\overline{F_1},\overline{F_2},...,\overline{F_{n-1}}))^{d_n}\times\det(m_{f_n}:A\longrightarrow A)$
ここで、$\overline{F_i}:=F_i(x_1,x_2,...,x_{n-1},0)$,$f_i:=F_i(x_1,x_2,...,x_{n-1},1)$（$i=1,2,...,n$），
$A:=\overline{k}[x_1,x_2,...,x_{n-1}])/<f_1,f_2,...,f_{n-1}>$,$\overline{k}$ は k の代数的閉体とする。

定理 4 を $\mathrm{Res}_{m,m,...,m}(x_n^{m-m_1}H_1,H_2,...,H_n)$ に使うと以下のように式変形ができる。$\mathrm{Res}_{m,m,...,m}(x_n^{m-m_1}H_1,H_2,...,H_n)$
$=\mathrm{Res}_{m,m,...,m}(\overline{H_2},...,\overline{H_n})^m\times\det(m_{h_1}:A\longrightarrow A)$
ここで、$\overline{H_i}:=H_i(x_1,x_2,...,x_{n-1},0)$,$h_i:=H_i(x_1,x_2,...,x_{n-1},1)(i=1,2,...,n)$，
$A:=\overline{k}[x_1,x_2,...,x_{n-1}]/<h_2,h_3,...,h_{n-1}>$ とする。
$m=(m-m_1)+m_1$ と書くことで、さらに以下のように式変形ができる。

$\mathrm{Res}_{m,m,...,m}(x_n^{m-m_1}H_1,H_2,...,H_n)$
$=\mathrm{Res}_{m,...,m}(\overline{H_2},...,\overline{H_n})^m\times\det(m_{h_1}:A\longrightarrow A)$
$=\mathrm{Res}_{m,...,m}(\overline{H_2},...,\overline{H_n})^{(m-m_1)+m_1}\times\det(m_{h_1}:A\longrightarrow A)$
$=\mathrm{Res}_{m,...,m}(\overline{H_2},...,\overline{H_n})^{(m-m_1)}\times\mathrm{Res}_{m,m,...,m}(\overline{H_2},...,\overline{H_n})^{m_1}$
$\times\det(m_{h_1}:A\longrightarrow A)$

$\mathrm{Res}_{m,...,m}(\overline{H_2},...,\overline{H_n})^{m_1}\times\det(m_{h_1}:A\longrightarrow A)$ に再度定理 4 を使うことによって、
$\mathrm{Res}_{m,...,m}(\overline{H_2},...,\overline{H_n})^{m_1}\times\det(m_{h_1}:A\longrightarrow A)=\mathrm{Res}_{m_1,m,...,m}(H_1,H_2,...,H_n)$
が成り立ち、定理 1 の後半が示された。

定理 1 を使う場合と使わない場合の計算量および計算の早さの違いについて

[6] の 3 章定理 4.9 によると、（多変数）終結式は必ず 2 つの行列式の商として表せるので、
定理を使う場合と使わない場合のそれぞれについて、考えなければならない分子の行列式の大きさの違いを、変数の数ごとに以下で述べていく。
(1)$n=2$ のとき

$\mathrm{Res}_{d_1,d_2m}(F_1(h_1,h_2)^h, F_2(h_1,h_2)^h)$
$= \mathrm{Res}_{d_1,d_2}(F_1,F_2))^m \times (\mathrm{Res}_{m,m}(x_2^{m-m_1}H_1, H_2)^{d_1d_2}$
$= \mathrm{Res}_{d_1,d_2}(F_1,F_2)^m \times (\mathrm{Res}_{m_1,m}(H_1,H_2))^{d_1d_2} \times (\mathrm{Res}_m(\overline{H_2}))^{d_1d_2(m-m_1)}$
$(m_1 < m)$
が成り立つが、
定理の 1 つ目の等号でどれくらい行列式の大きさが変わってくるかを見る。
定理を使う前だと、考えなければならない行列式の大きさは $d_1m + d_2m$ であり、
定理の 1 つ目の等号を使うことで、考えなければならない行列式の大きさは、$d_1 + d_2$ と $m + m$ まで小さくなる。
定理の 2 つ目の等号を使うことで、考えなければならない行列式の大きさは、さらに $d_1 + d_2$ と $m_1 + m$ まで小さくなる。m_1 と m の大きさに差が無いとき、2 つめの等号を使っても計算量に大きな違いが出ないが、m_1 と m が大きく異なるとき ($m_1 \ll m$ のとき)、2 つめの等号を使うことで計算量が大きく違ってくる。
具体的な例を用いて考えてみる。
$d_1 + d_2 \in \{16, 17, 18, 19, 20\}$、$m_1 = 1$、$m \in \{16, 17, 18, 19, 20\}$ なる d_1, d_2, m_1, m について
計算量を以下にまとめていく。(※ $d_1, d_2 > 0$ とする。)

まず、定理を使わない場合の行列式の大きさを以下の表にまとめる。

$m \backslash d_1 + d_2$	16	17	18	19	20
16	256	272	288	304	320
17	272	289	306	323	340
18	288	306	324	342	360
19	304	323	342	361	380
20	320	340	360	380	400

次に定理の 1 つ目の等号を使う場合の行列式の大きさを以下にまとめる。

$m \backslash d_1 + d_2$	16	17	18	19	20
16	16,32	17,32	18,32	19,32	20,32
17	16,34	17,34	18,34	19,34	20,34
18	16,36	17,36	18,36	19,36	20,36
19	16,38	17,38	18,38	19,38	20,38
20	16,40	17,40	18,40	19,40	20,40

(※ Res_{d_1,d_2} の行列式の大きさ,$\mathrm{Res}_{m,m}$ の行列式の大きさの順に記している。)

最後に定理の 2 つめの等号を使う場合の行列式の大きさを以下にまとめる。

$m \backslash d_1 + d_2$	16	17	18	19	20
16	16,17	17,17	18,17	19,17	20,17
17	16,18	17,18	18,18	19,18	20,18
18	16,19	17,19	18,19	19,19	20,19
19	16,20	17,20	18,20	19,20	20,20
20	16,21	17,21	18,21	19,21	20,21

(※ Res_{d_1,d_2} の行列式の大きさ,$\mathrm{Res}_{m,m}$ の行列式の大きさの順に記している。)

定理を使うことで、最終的に行列式の大きさは 20 以下になることが分かる。
実際に
$F_1 := y_1^5 + y_1^3y_2^2 + y_2^5$
$F_2 := y_1^{15} + y_1^5y_2^{10} + y_2^{15}$
$H_1 := x_1 + x_2$
$H_2 := x_1^{20} + x_1^{14}x_2^6 + x_1^{10}x_2^{10} + x_1^8x_2^{12} + x_1^6x_2^{14} + x_1^4x_2^{16} + x_1^2x_2^{18} + x_2^{20}$
$((d_1, d_2) = (5, 15), (m_1, m) = (1, 20))$

としてプロセッサー速度 2.6GHz、メインメモリ量 8GB の PC 上の mathematica 8 を使って計算してみたところ、定理を使わずに計算すると（すなわち $\mathrm{Res}_{d_1m,d_2m}(F_1(h_1,h_2)^h, F_2(h_1,h_2)^h)$ を直接計算。Det コマンドを使って、400 × 400 行列の行列式を計算。※詳しいコマンドの内容は付録を参照。）、計算に要した時間は 6.02 秒だった一方で、定理を使って計算すると（すなわち $\mathrm{Res}_{d_1,d_2}(F_1,F_2)$ と $\mathrm{Res}_{m_1,m}(H_1,H_2)$ を計算。Det コマンドを使って、20 × 20 と 21 × 21 の行列式を計算。※詳しいコマンドの内容は付録を参照。）、計算に要した時間は 0.01 秒だった。
また、論文 [7] によると、大きさが 250〜400 の行列式の計算には、14,341,734〜58,053,434 回の乗算・加減算・除算が必要な一方で、大きさが 20 の行列式の計算には、7,960 回の乗算・加減算・除算しか必要でない。
したがって、定理を使うことで、考えなければならない行列式の大きさが減り、行列式の大きさが減ることで、計算時間・計算量が減ることが分かる。

(2)$n = 3$ のとき

$\mathrm{Res}_{d_1m,d_2m,d_3m}(F_1(h_1,h_2,h_3)^h, F_2(h_1,h_2,h_3)^h, F_3(h_1,h_2,h_3)^h)$
$= \mathrm{Res}_{d_1,d_2,d_3}(F_1,F_2,F_3)^{m^2} \times \mathrm{Res}_{m,m,m}(x_3^{m-m_1}H_1, H_2, H_3)$
$= \mathrm{Res}_{d_1,d_2,d_3}(F_1,F_2,F_3)^{m^2} \times \mathrm{Res}_{m_1,m,m}(H_1,H_2,H_3)^{m^2} \times \mathrm{Res}_{m,m}(\overline{H}_2, \overline{H}_3)$
が成り立つが、
定理の 1 つ目の等号でどれくらい行列式の大きさが変わってくるかを見る。
定理を使う前だと、考えなければならない行列式の大きさは、${}_{d_1m+d_2m+d_3m}C_2$ であり、
定理の 1 つ目の等号を使うことで、考えなければならない行列式の大きさは、${}_{d_1+d_2+d_3}C_2$ と ${}_{m+m+m}C_2$ まで小さくなる。
定理の 2 つ目の等号を使うことで、考えなければならない行列式の大きさは、さらに ${}_{d_1+d_2+d_3}C_2$、${}_{m_1+m+m}C_2$ と ${}_{m+m}C_1 = m + m$ まで小さくなる。
具体的な例を用いて考えてみる。
$d_1 + d_2 + d_3 \in \{6, 7, 8, 9, 10\}$、$m_1 = 1$、$m \in \{1, 2, 3, 4, 5\}$ なる d_1, d_2, d_3, m_1, m について
計算量の違いを以下にまとめていく。

まず、定理を使わない場合の行列式の大きさを以下の表にまとめる。

$m \backslash d_1 + d_2 + d_3$	6	7	8	9	10
1	15	21	28	36	45
2	66	91	120	153	190
3	153	210	276	351	435
4	276	378	496	630	780
5	435	595	780	990	1225

次に定理の 1 つ目の等号を使う場合の行列式の大きさを以下にまとめる。

$m \backslash d_1 + d_2 + d_3$	6	7	8	9	10
1	15, 3	21, 3	28, 3	36, 3	45, 3
2	15, 15	21, 15	28, 15	36, 15	45, 15
3	15, 36	21, 36	28, 36	36, 36	45, 36
4	15, 66	21, 66	28, 66	36, 66	45, 66
5	15, 105	21, 105	28, 105	36, 105	45, 105

（※ $\mathrm{Res}_{d_1,d_2,d_3}$ の行列式の大きさ,$\mathrm{Res}_{m,m}$ の行列式の大きさの順に記している。）

最後に定理の 2 つめの等号を使う場合の行列式の大きさを以下にまとめる。

$m \backslash d_1 + d_2$	6	7	8	9	10
1	15, 3	21, 3	28, 3	36, 3	45, 3
2	15, 10	21, 10	28, 10	36, 10	45, 10
3	15, 21	21, 21	28, 21	36, 21	45, 21
4	15, 36	21, 36	28, 36	36, 36	45, 36
5	15, 55	21, 55	28, 55	36, 55	45, 55

（※ Res_{d_1,d_2} の行列式の大きさ,$\mathrm{Res}_{m,m}$ の行列式の大きさの順に記している。）
定理を使うことで最終的に行列式の大きさは、60 以下にまで小さくなる。
d_1, d_2, d_3, m_1, m の値がさらに大きくなると、定理を使うことによりさらに行列式を小さくすることができると考えられる。

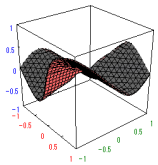
$(3)n = p$ のとき
$\mathrm{Res}_{d_1 m, d_2 m, ..., d_p m}(F_1(h_1, h_2, ..., h_p)^h, F_2(h_1, h_2, ..., h_p)^h, ..., F_p(h_1, h_2, ..., h_p)^h)$
$= \mathrm{Res}_{d_1, d_2, ..., d_p}(F_1, F_2, ..., F_p)^{m^{p-1}} \times \mathrm{Res}_{m,m,...,m}(x_p^{(m_1-m)} H_1, H_2, ..., H_p)^{d_1 d_2 ... d_p}$
$= \mathrm{Res}_{d_1, d_2, ..., d_p}(F_1, F_2, ..., F_p)^{m^{p-1}} \times \mathrm{Res}_{m_1,m,...,m}(H_1, H_2, ..., H_p)^{d_1 d_2 ... d_p}$
$\times \mathrm{Res}_{m,...,m}(\overline{H}_2, ..., \overline{H}_p)$
が成り立つが、
定理の 1 つ目の等号でどれくらい行列式の大きさが変わってくるかを見る。
定理を使う前だと、考えなければならない行列式の大きさは、${}_{d_1 m + d_2 m + ... + d_p m}C_{p-1}$ であり、
定理の 1 つ目の等号を使うことで、考えなければならない行列式の大きさは、${}_{d_1+d_2+...+d_p}C_{p-1}$ と ${}_{m+m+...+m}C_{p-1}$ まで小さくなる。
定理の 2 つ目の等号を使うことで、考えなければならない行列式の大きさは、${}_{d_1+d_2+...+d_p}C_{p-1}$、${}_{m_1+m+...+m}C_{p-1}$ と ${}_{m+...+m}C_{p-2}$ まで小さくなる。

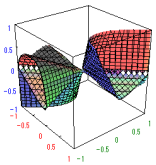
定理 1 を使うことで、共通零点を持つことが分かる図形の紹介

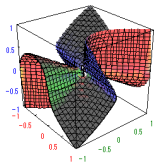
実数係数の 3 変数多項式の場合を考える。
定理 2 を使うと、以下が成り立つ。
$F_1(x_1, x_2, x_3)$,$F_2(x_1, x_2, x_3)$,$F_3(x_1, x_2, x_3) \in \mathbf{R}[x_1, x_2, x_3]$
（$F_1(x_1, x_2, x_3)$,$F_2(x_1, x_2, x_3)$,$F_3(x_1, x_2, x_3)$）の次数はそれぞれ d_1,d_2,d_3 とする。）
について
$\mathrm{Res}_{d_1,d_2,d_3}(F_1, F_2, F_3) = 0$
$\iff F_1 = F_2 = F_3 = 0$ は $\overline{\mathbf{R}^3} \setminus \{0\} = \mathbf{C}^3 \setminus \{0\}$ に解を持つ。
$\iff$（その解が $\mathbf{R}^3$ にあるとき、）曲線 $F_1 = 0$ と曲線 $F_2 = 0$ と曲線 $F_3 = 0$ は $\mathbf{R}^3$ に交点を持つ。
したがって、$F_1(H_1, H_2, H_3)$,$F_2(H_1, H_2, H_3)$,$F_3(H_1, H_2, H_3)$
（ここで F_1,F_2,F_3 は先と同様のもの,H_1,H_2,$H_3 \in \mathbf{R}[x_1, x_2, x_3]$ の次数はそれぞれ m_1,m,m（$m_1 < m$）とする。）
についても同様に、
曲線 $F_1(h_1, h_2, h_3)^h = 0$、曲線 $F_2(h_1, h_2, h_3)^h = 0$、曲線 $F_3(h_1, h_2, h_3)^h = 0$ は $\mathbf{R}^3 \setminus 0$ に交点を持つ。
$\iff F_1(h_1, h_2, h_3)^h = F_2(h_1, h_2, h_3)^h = F_3(h_1, h_2, h_3)^h = 0$ は $\mathbf{R}^3 \setminus 0$ に解を持つ。
$\iff \mathrm{Res}_{d_1 m_1, d_2 m, d_3 m}(F_1(h_1, h_2, h_3)^h, F_2(h_1, h_2, h_3)^h, F_3(h_1, h_2, h_3)^h) = 0$
$\iff \mathrm{Res}_{d_1,d_2,d_3}(F_1, F_2, F_3) = 0$ または $\mathrm{Res}_{m_1,m,m}(H_1, H_2, H_3) = 0$ または $\mathrm{Res}_{m,m}(\overline{H_2}, \overline{H_3}) = 0$
（$\because \mathrm{Res}_{d_1 m, d_2 m_2, d_3 m_3}(F_1(h_1, h_2, h_3)^h, F_2(h_1, h_2, h_3)^h, F_3(h_1, h_2, h_3)^h)$
$= (\mathrm{Res}_{d_1,d_2,d_3}(F_1, F_2, F_3))^{m^2} \times (\mathrm{Res}_{m,m,m}(x_3^{m-m_1} H_1, H_2, H_3))^{d_1 d_2 d_3}$
$= (\mathrm{Res}_{d_1,d_2,d_3}(F_1, F_2, F_3))^{m^2} \times (\mathrm{Res}_{m_1,m,m}(H_1, H_2, H_3))^{d_1 d_2 d_3})$
$\times (\mathrm{Res}_{m,m}(\overline{H_2}, \overline{H_3}))^{(m-m_1) d_1 d_2 d_3})$
$\iff$
$F_1 = F_2 = F_3 = 0$ は、$\mathbf{R}^3 \setminus 0$ に解を持つ。または $H_1 = H_2 = H_3 = 0$ は、$\mathbf{R}^3 \setminus 0$ に解を持つ。または $\overline{H_2} = \overline{H_3} = 0$ は、$\mathbf{R}^2 \setminus 0$ に解を持つ。
が成り立つ。

具体的な多項式を用いて考えてみる。

$F_1 := 2y_1 + y_2 - y_3$,$F_2 := y_1^2 - y_2^2 + y_3^2$,$F_3 := 4y_1^3 - 2y_2^3 + y_1y_2^2 + y_3^3$
$H_1 := x_1^2 + x_2^2 + x_3^2$,$H_2 := x_1^3 + x_1^2x_2 - x_1x_2^2 - x_2^3 + 2x_1x_3^2 + 3x_1^2x_3 + x_3^3$,
$H_3 := x_1^3 - 3x_1^2x_2 + 3x_1x_2^2 - x_2^3 + x_1^2x_3 + x_2^2x_3 + x_1x_2x_3 + 2x_3^3$
とすると、
・$F_1(h_1, h_2, h_3)^h$
$= (2h_1 + h_2 - h_3)^h$
$= 2x_3H_1 + H_2 - H_3$
$= 4x_1^2x_2 - 4x_1x_2^2 + 4x_1^2x_3 - x_1x_2x_3 + x_2^2x_3 + 2x_1x_3^2 + x_3^3$
・$F_2(h_1, h_2, h_3)^h$
$= (h_1^2 - h_2^2 + h_3^2)^h$
$= (x_3H_1)^2 - H_2^2 + H_3^2$
$= -8x_1^5x_2 + 16x_1^4x_2^2 - 16x_1^3x_2^3 + 16x_1^2x_2^4 - 8x_1x_2^5 - 4x_1^5x_3 - 10x_1^4x_2x_3 + 8x_1^3x_2^2x_3 + 4x_1^2x_2^3x_3 + 4x_1x_2^4x_3 - 2x_2^5x_3 - 11x_1^4x_3^2 - 2x_1^3x_2x_3^2 + 9x_1^2x_2^2x_3^2 + 6x_1x_2^3x_3^2 + 2x_2^4x_3^2 - 10x_1^3x_3^3 - 14x_1^2x_2x_3^3 + 14x_1x_2^2x_3^3 - 2x_2^3x_3^3 - 4x_1^2x_3^4 - 4x_1x_2x_3^4 + 6x_2^2x_3^4 - 4x_1x_3^5 + 4x_3^6$
・$F_3(h_1, h_2, h_3)^h$
$= (4h_1^3 - 2h_2^3 + h_1h_2^2 + h_3^3)^h$
$= 4\left(x_3H_1\right)^3 - 2H_2^3 + \left(x_3H_1\right)H_2^2 + H_3^3$
$= -x_1^9 - 15x_1^8x_2 + 36x_1^7x_2^2 - 68x_1^6x_2^3 + 138x_1^5x_2^4 - 138x_1^4x_2^5 + 68x_1^3x_2^6 - 36x_1^2x_2^7 + 15x_1x_2^8 + x_2^9 - 14x_1^8x_3 - 49x_1^7x_2x_3 + 48x_1^6x_2^2x_3 + 37x_1^5x_2^3x_3 + 46x_1^4x_2^4x_3 - 71x_1^3x_2^5x_3 + 12x_1^2x_2^6x_3 - 13x_1x_2^7x_3 + 4x_2^8x_3 - 57x_1^7x_3^2 - 75x_1^6x_2x_3^2 + 66x_1^5x_2^2x_3^2 + 96x_1^4x_2^3x_3^2 + 12x_1^3x_2^4x_3^2 - 30x_1^2x_2^5x_3^2 - 9x_1x_2^6x_3^2 - 3x_2^7x_3^2 - 107x_1^6x_3^3 - 111x_1^5x_2x_3^3 + 194x_1^4x_2^2x_3^3 - 21x_1^3x_2^3x_3^3 + 109x_1^2x_2^4x_3^3 - 47x_1x_2^5x_3^3 + 6x_2^6x_3^3 - 136x_1^5x_3^4 - 76x_1^4x_2x_3^4 + 78x_1^3x_2^2x_3^4 + 42x_1^2x_2^3x_3^4 + 22x_1x_2^4x_3^4 - 14x_2^5x_3^4 - 109x_1^4x_3^5 - 8x_1^3x_2x_3^5 + 72x_1^2x_2^2x_3^5 + 32x_1x_2^3x_3^5 + 18x_2^4x_3 - 64x_1^3x_3^6 - 40x_1^2x_2x_3^6 + 44x_1x_2^2x_3^6 - 8x_2^3x_3^6 - 7x_1^2x_3^7 + 12x_1x_2x_3^7 + 25x_2^2x_3^7 - 8x_1x_3^8 + 11x_3^9$
となり、これをらのグラフ 3 次元実空間上に以下のようになる。







$F_1(h_1, h_2, h_3)^h = 0$　　$F_2(h_1, h_2, h_3)^h = 0$　　$F_3(h_1, h_2, h_3)^h = 0$

一見これらの図形は共通零点を持つかどうかが分からないが、定理を使うことで、共通零点を持つことが分かる。
何故なら
$\overline{H}_2(x_1, x_2) = H_2(x_1, x_2, 0) = x_1^3 + x_1^2x_2 - x_1x_2^2 - x_2^3 = (x_1 - x_2)(x_1 + x_2)^2$
$\overline{H}_3(x_1, x_2) = H_3(x_1, x_2, 0) = x_1^3 - 3x_1^2x_2 + 3x_1x_2^2 - x_2^3 = (x_1 - x_2)^3$
であり、$\overline{H}_2(x_1, x_2) = \overline{H}_3(x_1, x_2) = 0$ は $(1, 1) \in \mathbf{R}^2 \setminus 0$ を解に持つ。
したがって定理 2 より、
$\mathrm{Res}_{3,3}(\overline{H}_2, \overline{H}_3) = 0$ となるので、主定理を使うことで
$\mathrm{Res}_{1\times2,2\times3,3\times3}(F_1(h_1, h_2, h_3)^h, F_2(h_1, h_2, h_3)^h, F_3(h_1, h_2, h_3)^h)$
$= \mathrm{Res}_{1,2,3}(F_1, F_2, F_3)^{3^2} \times \mathrm{Res}_{3,3,3}(x_3H_1, H_2, H_3)^{1\times2\times3}$
$= \mathrm{Res}_{1,2,3}(F_1, F_2, F_3)^{3^2} \times \mathrm{Res}_{2,3,3}(H_1, H_2, H_3)^{1\times2\times3} \times \mathrm{Res}_{3,3}(\overline{H}_2, \overline{H}_3)^{(3-2)\times(1\times2\times3)}$
$= 0$ となる。
再度定理 2 を使うと、$F_1(h_1, h_2, h_3)^h = F_2(h_1, h_2, h_3)^h = F_3(h_1, h_2, h_3)^h = 0$ は $\mathbf{R}^2 \setminus 0$ に解を持つからである。

論文 [2] の主定理の一般化

まず、[2] の主定理の紹介と、それを一般化した定理の紹介と、その定理の証明を行う。

定理 5

([2] から引用) $\mathrm{Res}_{m_1,c}(H_1,G_2)\neq 0$ かつ、$2|m_1$ のとき $\mathrm{Res}_{m_1,d_2c}(H_1,F_2(G_1,G_2))=\mathrm{Res}_{m_1,d_2}(\mathrm{Res}_{m_1,c}(H_1,y_2G_1-y_1G_2),F_2)$

ここで、H_1 は次数 m_1 の体 k 係数 2 変数 (x_1,x_2 を変数とする) 斉次多項式、F_2 は次数 d_2 の体 k 係数 2 変数 (y_1,y_2 を変数とする) 斉次多項式、G_1,G_2 は次数 c の体 k 係数 2 変数（x_1,x_2 を変数とする）斉次多項式とする。

定理 6

$\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_2)\neq 0$ かつ、$2|m_1m_2...m_{n-1}$ のとき
$\mathrm{Res}_{m_1,m_2,...,m_{n-1},d_nc}(H_1,H_2,...,H_{n-1},F_n(G_1,G_2))$
$=\mathrm{Res}_{m_1,m_2,...,m_{n-1},d_n}(\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},y_2G_1-y_1G_2),F_n)$

ここで、$H_1,...,H_{n-1}$ は次数 $m_1,...,m_{n-1}$ の体 k 係数 n 変数 (x_1,x_2,...,x_n を変数とする) 斉次多項式、F_n は次数 d_n の体 k 係数 2 変数 (y_1,y_2 を変数とする) 斉次多項式、G_1,G_2 は次数 c の体 k 係数 n 変数 (x_1,x_2,...,x_n を変数とする) 斉次多項式とする。

定理 6 を証明するために、補題をひとつ用意する。

補題 7

$H_1,H_2,...,H_{n-1},G_1,G_2,m_1,m_2,...,m_{n-1},d$ の条件を定理 6 と同じものとする。
$\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_1-zG_2)\in k[z]$ の
z に関する先頭係数は $\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_2)$ となり、
$\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_1-zG_2)$ の次数は $e_1e_2...e_{n-1}$ となる。

＜証明＞ $p(z):=\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_1-zG_2)$ とおく。
[6] の 3 章定理 3.1 より、$p(z)$ を、
$p(z)\in\mathbf{Z}[\{H_1,H_2,...,H_{n-1},G_1-zG_2\text{の係数}\}][z]$ と見なしたとき、
$p(z)$ の、変数 G_1-zG_2の係数 における次数は $m_1m_2...m_{n-1}$ となる。
したがって、$deg_zp(z)\leqq m_1m_2...m_{n-1}$ となる。
ここで、$p^h(y_1,y_2):=y_2^{m_1m_2...m_{n-1}}\times p(\frac{y_1}{y_2})$（つまり、$p^h$ は p を斉次化させた多項式）とおくと、$p^h(1,0)\neq 0$ のとき、$p(z)$ の次数は $m_1m_2...m_{n-1}$ であり、その先頭係数は $p^h(1,0)$ となる。
したがって、$p^h(1,0)=\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_2)$ となることを示せばよい。

$$\begin{aligned}p^h(1,0)&=\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},0\times G_1-1\times G_2)\\&=\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},-G_2)\\&=(-1)^{m_1m_2...m_{n-1}}\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_2)\\&(\because\text{[6] の 3 章定理 3.1 より})\\&=\mathrm{Res}_{m_1,m_2,...,m_{n-1}}(H_1,H_2,...,H_{n-1},g_2)\\&(\because 2|m_1m_2...m_{n-1}\text{より})\end{aligned}$$

以上より、補題 7 が示された。

定理 6 の証明

$\mathrm{Res}_{m_1,m_2,...,m_{n-1},d_nc}(H_1,H_2,...,H_{n-1},F_n(g_1,g_2))$

$=\mathrm{Res}_{m_1,m_2,...,m_{n-1}}(\overline{H_1},\overline{H_2},...,\overline{H_{n-1}})^{d_nc}\times \prod_{a\in\mathbf{V}(h_1,h_2,...,h_{n-1})} F_n(g_1(a),g_2(a))$

（ここで、$\overline{H_i}:=H_i(x_1,x_2,...,x_{n-1},0)$、$h_1:=H_i(x_1,x_2,...,x_{n-1},1)$、$g_i=G_i(x_1,x_2,...,x_{n-1},1)$ とおく）

$=\mathrm{Res}_{m_1,m_2,...,m_{n-1}}(\overline{H_1},\overline{H_2},...,\overline{H_{n-1}})^{d_nc}\times \prod_{1\leqq i\leqq p} F_n(g_1(a_i),g_2(a_i))$

（ここで、$\mathbf{V}(h_1,h_2,...,h_{n-1}):=\{a_1,a_2,...,a_p\}$ $(p<\infty)$ とおく）

$=\mathrm{Res}_{m_1,m_2,...,m_{n-1}}(\overline{H_1},\overline{H_2},...,\overline{H_{n-1}})^{d_nc}\times \prod_{1\leqq i\leqq p} g_2(a_i)^{d_n}$

$\times \prod_{1\leqq i\leqq p} F_n(\frac{g_1(a_i)}{g_2(a_i)},1)$

（※ $\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_2)\neq 0$ より、$g_2(a_i)\neq 0$）

$=\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_2)^{d_n}\times \prod_{1\leqq i\leqq p} F_n(\frac{g_1(a_i)}{g_2(a_i)},1)$

ある i について $b_i=\frac{g_1(a_i)}{g_2(a_i)}$ おく。

すると、b_i は $g_1(a_i)-b_ig_2(a_i)=0$ をみたす。

$g_1(a_i)-b_ig_2(a_i)=0$

$\Longleftrightarrow \prod_{1\leqq i\leqq p}(g_i(a_i)-b_ig_2(a_i))=0$

$\Longleftrightarrow \mathrm{Res}_{m_1,m_2,...,m_{n-1}}(\overline{H_1},\overline{H_2},...,\overline{H_{n-1}})\times \prod_{1\leqq i\leqq p}(g_i(a_i)-b_ig_2(a_i))=0$

$\Longleftrightarrow \mathrm{Res}_{m_1,m_2,...,m_{n-1}}(H_1,H_2,...,H_{n-1},G_1-b_iG_2)=0$

となるので、

$\prod_{1\leqq i\leqq p} F_n(\frac{g_1(a_i)}{g_2(a_i)},1)$

$=\prod_{1\leqq i\leqq p} F_n(b_i,1)$

$=\prod_{b:\mathrm{Res}(H_1,H_2,...,H_{n-1},G_1-bG_2)=0} F_n(b,1)$

と書き換えることができる。

したがって

$\mathrm{Res}_{m_1,m_2,...,m_{n-1}}(H_1,H_2,...,H_{n-1},F_n(G_1,G_2))$

$=\mathrm{Res}_{m_1,m_2,...,m_{n-1}}(H_1,H_2,...,H_{n-1},G_2)^{d_n}\times \prod_{b:\mathrm{Res}(H_1,H_2,...,H_{n-1},G_1-bG_2)=0} F_n(b,1)$

$$=\mathrm{Res}_{m_1,m_2,...,m_{n-1}}(H_1,H_2,...,H_{n-1},G_2)^{d_n}\times\frac{\mathrm{Res}(\mathrm{Res}(H_1,H_2,...,H_{n-1},G_1-zG_2),F_n(z,1))}{(\mathrm{Res}(H_1,H_2,...,H_{n-1},G_1-zG_2)\text{ の先頭係数})^{d_n}}\qquad(1)$$

$=\mathrm{Res}_{m_1m_2...m_{n-1},d_n}(\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},G_1-zG_2),F_n(z,1))$

$=\mathrm{Res}_{m_1m_2...m_{n-1},d_n}(\mathrm{Res}_{m_1,m_2,...,m_{n-1},c}(H_1,H_2,...,H_{n-1},y_2G_1-y_1G_2),F_n(y_1,y_2)$

以上より、定理 6 が証明された。

参考文献

[1] Manfred Minimair.(2002).”Dense Resultant of composed polynomial Mixed-mixed case. ”J. Symb. Comput. 36, 825-834

[2] Manfred Minimair.(2005). ”Resultant of partially composed polynomials. ”J. Symb. Comput. 41, 591-602

[3] I. Gelfand, M. Kapranov and A. Zelevinsky. (1994). ”Discriminants, Resultants and Multidimensional determinants. ”, Boston, Birkhauser

[4] CHARLES CHING-AN CHENG, JAMES H. MCKAY, AND STUART SUI-SHENG WANG. (1992). ”A CHAIN RULE FOR MULTIVARIABLE RESULTANTS. ”Proc.Amer.Math.Soc.123(4),1037-1047

[5] J. Jouanolou. (1991). ”Le formalisme du Resultant. ”Advances in Math. 90, 117-263

[6] Cox,D., Little, J., O'Shea, D. (1998). "Using Algebraic Geometry. "New York, Springer

[7] 木下　孝, 牧野潔夫, 三好和憲 (1995)"Fraction-free による行列式の計算効率"数理解析研究所講究録 920 巻,62-73