数理解析研究所講究録 1324 巻 2003 年 207-216

5 次可移群に対する $\boldsymbol{Q}$ 上 2 助変数生成的多項式の構成
(A construction of generic polynomials with two parameters over $\boldsymbol{Q}$ for the transitive groups of degree 5)

早大理工 (Waseda Univ) 橋本 喜一朗 (HASHIMOTO Ki-ichiro)
上智理工 (Sophia Univ.) 角皆 宏 (TSUNOGAI Hiroshi)

0. 概要

5 次対称群 $\mathfrak{S}_5$ の可移部分群は次の 5 種である。

5 次巡回群	C_5	$\simeq$	$\boldsymbol{Z}/5\boldsymbol{Z}$	位数	5
5 次二面体群	D_5	$\simeq$	$\{\pm 1\} \ltimes \boldsymbol{Z}/5\boldsymbol{Z}$		10
Frobenius 群	$F_{20} = F_{5,4}$	$\simeq$	$(\boldsymbol{Z}/5\boldsymbol{Z})^\times \ltimes \boldsymbol{Z}/5\boldsymbol{Z}$		20
5 次交代群	$\mathfrak{A}_5$				60
5 次対称群	$\mathfrak{S}_5$				120

本稿では、順番付 5 標点射影直線のモジュライ空間 $\mathcal{M}_{0,5}$ への 5 次対称群 $\mathfrak{S}_5$ の作用の考察により、これら全ての 5 次可移群に対し、有理数体 $\boldsymbol{Q}$ 上の 2 助変数生成的多項式を構成する。このような多項式は夫々の場合に対し既に知られているが、この方法では、同じ道具立てから全ての場合の構成ができ、幾つかの場合 (特に 5 次交代群 $\mathfrak{A}_5$ の場合) には従来のものより遥かに簡単な係数の多項式が得られた。又、このように幾何的な意味が明快な道具立てを用いたことの応用として、5 次の Nöther 問題の別証明が得られたことにも触れる。

1. 生成的多項式

Galois の逆問題 (構成問題) とは、

問題. 与えられた体 K 及び有限群 G に対し、$\mathrm{Gal}(L/K) \simeq G$ となる体拡大 L/K が存在するか。存在するなら体 L (より具体的には K 上の分解体が L となる G-多項式 $f(X) \in K[X]$) を構成せよ。

というものであるが、更に自然に欲張って「一つの拡大 (多項式) から全ての G-拡大を与えることができないか」ということで生成的拡大や生成的多項式の概念に行き着く (Saltman [Sa], DeMeyer [DM] 他)。

定義. 体 k 及び有限群 G に対し、$f(\boldsymbol{t}; X) \in k(\boldsymbol{t})[X] = k(t_1, \ldots, t_n)[X]$ が次を満たすとき、G に対する k 上 n 助変数の**生成的多項式 (generic polynomial)** であるという。

(1) 関数体上 G-多項式である。即ち、L を $k(\boldsymbol{t})$ 上の f の分解体とする時、$\mathrm{Gal}(L/k(\boldsymbol{t})) \simeq G$。

京大数研講究録原稿.

(2) k 上生成的である。即ち、$\mathrm{Gal}(L/K) \simeq G$ となる任意の体拡大 $L \supset K \supset k$ に対し、L が K 上の $f(\boldsymbol{a}; X)$ の分解体となるような $\boldsymbol{a} = (a_1, \ldots, a_n) \in K^n$ が存在する。 ▮

生成的多項式に関しては一般に次のような問題が考えられる。

<u>問題</u>．

(1) 与えられた体 k と有限群 G とに対し、生成的多項式が存在するや否や。
(2) 存在するなら構成せよ。係数がなるべく簡単なものが望ましい。
(3) 助変数は最低でも幾つ必要か。少ない方が望ましい。 ▮

(1) が既に非自明な問題であり、実際、例えば $k = \boldsymbol{Q}, G = C_8$ の場合には生成的多項式が (助変数を増やしても) 存在しないことが知られている (Wang [Wa], Lenstra [Len])。又、(3) については、Buhler-Reichstein により定義された本質的次元 (essential dimension) $\mathrm{ed}_k G$ が下限の一つを与える ([BR1])。例えば、本稿で扱う 5 種の群 G に対しては、その $\boldsymbol{Q}$ 上の本質的次元 $\mathrm{ed}_{\boldsymbol{Q}} G$ は 2 であり、従って $\boldsymbol{Q}$ 上の 1 助変数の生成的多項式は存在しないことが知られている ([BR1, JLY])。しかし一般には $\mathrm{ed}_k G$ が決定されている例は少なく、例えば $\mathrm{ed}_{\boldsymbol{Q}} \mathfrak{S}_7$ は 3 か 4 であるが、そのどちらであるかは知られていない。

2. 従来の結果

既に 19 世紀に Hermite [Her] は、不変式論を用いて、一般 5 次方程式が

$$f(a, b; X) = X^5 + aX^3 + bX + b \tag{2.1}$$

の形に変形できることを示している。この結果を現代流に解釈すると、$f(a, b; X)$ が $\boldsymbol{Q}$ 上の生成的多項式であると理解でき、Coray [Co] はこの結果を基礎体の考察付きで再証明している。

上記 $f(a, b; X)$ の判別式を $D = D(a, b)$ とするとき、D を完全平方式とする a, b の 2 助変数表示を与えることにより、$f(a, b; X)$ から $\boldsymbol{Q}$ の生成的 $\mathfrak{A}_5$-多項式を得ることが出来るが、この方法で得られる多項式は係数が余り簡単でない。

Brumer [Br] は $\boldsymbol{Q}(\sqrt{5})$-実乗法をもつ種数 2 の曲線の考察により、3 助変数で 6 次の $\mathfrak{A}_5$-多項式族を構成した。この多項式族を更に特殊化することにより、2 助変数で $\boldsymbol{Q}$ 上生成的な 5 次の D_5 多項式族が得られる。後者は楕円曲線の 5 等分点を用いた方法で Mestre により見いだされていたものと同一である。橋本 [Has1, Has2] はこれらの族の別解釈による再構成と、生成性の再証明を与えた。この多項式に更に別の幾何的構成が与えられるというのが本研究の動機であった。実際、本稿の D_5-多項式はこの多項式の再々構成である。

Lecacheux [Lec] は楕円曲線の 5 等分点の考察を更に進めて、2 助変数で $\boldsymbol{Q}$ 上生成的な $F_{5,4}$-多項式を得た。本稿の方法でもこの多項式が再構成出来た。又、生成的ではないが $\boldsymbol{Q}$ 上の 1 助変数の C_5-多項式も得ている。

Buhler-Reichstein [BR2] ([JLY] 参照) は、$\boldsymbol{Q}(\zeta_5)$ 上の 5 次 Kummer 拡大を $\boldsymbol{Q}$ 上に降下させることにより、2 助変数で $\boldsymbol{Q}$ 上生成的な C_5-多項式を得たが、今回得られたものより係数が非常に複雑である。

3. Nöther 問題

本来の Nöther 問題とは次のものである。

問題．体 k 上の n 変数有理関数体 $K=k(t_1,\ldots,t_n)$ に n 次対称群 $\mathfrak{S}_n$ が変数の置換で作用している時、$\mathfrak{S}_n$ の可移部分群 G に対し、固定体 K^G は k 上有理的 (純超越的) であるか。 ▮

これが肯定的である時、$K^G=k(s_1,\ldots,s_n)$ とすれば、K を分解体とする K^G 上の多項式 $f(s_1,\ldots,s_n;X)\in K^G[X]$ は、n 助変数の k 上生成的 G-多項式である。

ここではこれを一般化した次の問題 (一般 Nöther 問題) を考える。

問題．体 k 上の n 変数有理関数体 $K=k(t_1,\ldots,t_n)$ に有限群 G が作用している時、固定体 K^G は k 上有理的であるか。 ▮

Nöther 問題は次の Lüroth 型の問題の特殊な場合でもある。

問題．体 k 上の n 変数有理関数体 $K=k(t_1,\ldots,t_n)$ に対し、k を含む K の部分体は有理的であるか。 ▮

$n=1$ の場合に肯定的であるというのが Lüroth の定理であり、$n=2$ の場合は k が標数 0 の代数閉体ならば Zariski-Castelnuovo の定理により肯定的である。

以下本稿では、$\boldsymbol{Q}$ 上の 2 変数有理関数体 $K=\boldsymbol{Q}(x,y)$ に、次節で導入する 5 次対称群 $\mathfrak{S}_5$ の作用を考え、$\mathfrak{S}_5$ の各可移部分群 G に対し、K^G 上の分解体が K となる多項式を構成する。この係数の間の関係を具体的に求めることにより K^G の有理性を示すと共に、我々の $\mathfrak{S}_5$ の作用の定義から生成性が従うことを示す。実際の計算には Maple や Mathematica を用いた。閉体上ではないので、有理性自体が自明ではないことに注意する。生成的多項式の定義で有理関数体上の多項式としたことは一見自然であるが、実際の構成ではこの点が最も非自明かつ困難なのであった。

4. $\mathcal{M}_{0,5}$ への $\mathfrak{S}_5$ 作用

順番付 5 標点射影直線のモジュライ空間を $\mathcal{M}_{0,5}$ とする。

$$\begin{aligned}\mathcal{M}_{0,5}&=\left((\mathbf{P}^1)^5\setminus(\text{weak diagonal})\right)/\mathrm{PGL}(2)\\&=\{(x_1,\ldots,x_5)\,|\,x_i\in\mathbf{P}^1,x_i\neq x_j(i\neq j)\}/\mathrm{PGL}(2),\end{aligned}\tag{4.1}$$

ここに $\mathrm{PGL}(2)=\mathrm{Aut}(\mathbf{P}^1)$ は対角作用。$(x_1,\ldots,x_5)$ の類を $[x_1,\ldots,x_5]$ で表す。関数体 $K:=\boldsymbol{Q}(\mathcal{M}_{0,5})=\boldsymbol{Q}(x_1,\ldots,x_5)^{\mathrm{PGL}(2)}$ は $\boldsymbol{Q}$ 上超越次元 2 の純超越拡大 (2 変数有理関数体) で複比 $\dfrac{x_i-x_k}{x_i-x_l}\Big/\dfrac{x_j-x_k}{x_j-x_l}$ で生成される。5 次対称群 $\mathfrak{S}_5$ は置換により $\mathcal{M}_{0,5}$ に左作用する。

$$\sigma\cdot[x_1,\ldots,x_5]:=[x_{\sigma^{-1}(1)},\ldots,x_{\sigma^{-1}(5)}]\qquad(\sigma\in\mathfrak{S}_5),\tag{4.2}$$

又、関数体 K にも $\sigma\cdot\varphi:=\varphi\circ\sigma^{-1}$ $(\sigma\in\mathfrak{S}_n,\varphi\in K)$ で忠実に左作用する。これを 2 変数有理関数体への作用として具体的に書き下そう。$\mathcal{M}_{0,5}$ の点 $P=[x_1,\ldots,x_5]$ は PGL(2)-作用により $[0,xy,x,1,\infty]$ の形に一意に書ける。この時、

$$x=\frac{x_3-x_1}{x_3-x_5}\Big/\frac{x_4-x_1}{x_4-x_5},\qquad y=\frac{x_2-x_1}{x_2-x_5}\Big/\frac{x_3-x_1}{x_3-x_5}\tag{4.3}$$

は $\mathcal{M}_{0,5}$ 上の関数と見做せ、これにより $\mathcal{M}_{0,5}=\left((\mathbf{P}^1\setminus\{0,1,\infty\})\right)^2\setminus\{xy=1\}$、及び $K=\boldsymbol{Q}(\mathcal{M}_{0,5})=\boldsymbol{Q}(x,y)$ となる。5 次対称群 $\mathfrak{S}_5$ の $\boldsymbol{Q}(x,y)$ への作用は次のようにして書き下せる。

例．$\alpha=(1\,2\,3\,4\,5)$ の作用を考えよう。$P=[x_1,\ldots,x_5]=[0,xy,x,1,\infty]$ に対し、$\alpha^{-1}(P)=[x_2,x_3,x_4,x_5,x_1]=[xy,x,1,\infty,0]=[0,1-y,1-xy,1,\infty]$ ($\xi\mapsto\dfrac{\xi-xy}{\xi}$ で再正規化) であるので、

$$\alpha:\begin{cases}x\longmapsto 1-xy\\ y\longmapsto\dfrac{1-y}{1-xy}\end{cases}\tag{4.4}$$ ∎

以下では、各 G に対し、分解体が K となるような多項式 $f^G(X)\in K^G[X]$ を作り、この $f^G[X]$ から $\boldsymbol{Q}$ 上の生成的多項式を構成する。置換作用を縮約して $\mathfrak{S}_5$ の作用を作ったことが生成性には本質的であるが、前述のように、更に K^G が $\boldsymbol{Q}$ 上有理的であることも要す。

5. 二面体群 D_5 (位数 10)

$\alpha=(1\ 2\ 3\ 4\ 5),\beta=(1\ 3)(4\ 5)\in\mathfrak{S}_5$ とおくと、$D_5=\langle\alpha,\beta\rangle$ は 5 次二面体群で、数珠順列 $(1,2,3,4,5)$ の固定群である。α の $K=\boldsymbol{Q}(x,y)$ への作用は (4.4) で求めた。同様にして β の K への作用は

$$\beta:\begin{cases}x\longmapsto x\\ y\longmapsto\dfrac{1-y}{1-xy}\end{cases}\tag{5.1}$$

となる。x の D_5-軌道 S は

$$S=\mathrm{Orb}_{D_5}(x)=\left\{x,1-xy,y,\frac{1-y}{1-xy},\frac{1-x}{1-xy}\right\},\tag{5.2}$$

であり、$f(X):=\prod_{u\in S}(X-u)=:X^5+c_4X^4+c_3X^3+c_2X^2+c_1X+c_0\in K^{D_5}[X]$ とおくと、集合 S を保つ $\mathrm{Aut}(K/\boldsymbol{Q})$ の元が D_5 に限ることから、$K^{D_5}=K(c_0,\ldots,c_4)$ であり、$f(X)$ が K^{D_5} 上の D_5-多項式であることが判る。

定理 1. (1) D_5-固定体 $K^{D_5}=K(c_0,\ldots,c_4)$ は $\boldsymbol{Q}$ 上有理的 (2 次元純超越的) であり、実際 $K^{D_5}=\boldsymbol{Q}(a,b)$ である。ここに、

$$c_0=a,\quad c_1=b,\quad c_2=a^2-a-1-2b,\quad c_3=b-a-3,\quad c_4=a-3.$$

(2) (Brumer[Br], 橋本 [Has1, Has2] の多項式の再構成)

$$f^{D_5}(a,b;X):=X^5+(-3+a)X^4+(3+b-a)X^3+(-1-a-2b+a^2)X^2+bX+a$$

は $\boldsymbol{Q}$ 上の生成的 D_5-多項式である。 ∎

証明．(1) $c_0, \ldots, c_4$ を x, y で表すことにより、c_i 達の間の関係式は計算機により直接確かめられる。又、関係式 $u + \alpha(u)\alpha^{-1}(u) = 1$ $(\forall u \in S)$ をうまく用いれば、手計算で確かめることも困難ではない。

(2) $L \supset K \supset \boldsymbol{Q}$ を $\mathrm{Gal}(L/K) \simeq D_5$ であるような任意の体拡大とせよ。正規底定理により、$K[D_5]$-加群として $L \simeq K[D_5]$ であるので、D_5 の置換表現と同型な L の部分 $K[D_5]$-加群 $W = \bigoplus_{i=1}^{5} Kx_i$ (ここに $\sigma(x_i) = x_{\sigma(i)}$) が存在する。この x_i 達から (4.3) によって x, y を定め、更に定理にあるように $a = -\sum_{u\in S} u, b = \sum_{u,v\in S, u\neq v} uv$ により a, b を定めると $a, b \in K$ である。この時 $x \neq y$ であれば、D_5 は $f^{D_5}(a, b; X) \in K[X]$ の根の集合に望むように作用し、L は K 上の $f^{D_5}(a, b; X)$ の分解体となる。$x = y (= (-1 \pm \sqrt{5})/2)$ の時は、$x \neq y$ となるように W の取り方を適切に変える必要があるが、それには良く用いられる方法 ([JLY]) があり、可能である。 □

6. 巡回群 C_5 (位数 5)

D_5 の巡回部分群 $C_5 = \langle \alpha = (1\ 2\ 3\ 4\ 5) \rangle$ について、固定体 K^{C_5} の有理性を考える。K^{C_5} は $K^{D_5} = \boldsymbol{Q}(a, b)$ の 2 次拡大である (a, b は定理 1 参照)。

$c = \prod_{i \in \boldsymbol{Z}/5\boldsymbol{Z}} (\alpha^i(x) - \alpha^{i+1}(x)) = \prod_{u \in S} (u - \alpha(u))$ とおくと、$\alpha(c) = c, \beta(c) = -c$ であるので、$K^{C_5} = K^{D_5}(c) = \boldsymbol{Q}(a, b, c), c^2 \in K^{D_5}$ である。c^2, a, b を x, y で書き下して計算することにより、次の関係式を得る。

$$
\begin{aligned}
(6.1)\quad H(a,b,c) := {}& c^2 + 4b^3 + (-a^2 + 30a - 1)b^2 \\
& + (-24a^3 + 34a^2 + 14a)b + (4a^5 - 4a^4 - 40a^3 + 91a^2 - 4a) = 0
\end{aligned}
$$

注．(6.1) は、特異点を有する $\mathbf{P}_a^1$ 上の楕円曲面を与える。楕円曲面の理論によっても、(6.1) は $\overline{\boldsymbol{Q}}$ 上有理的であることが判るが、我々の問題の重大な所は $\boldsymbol{Q}$ 上有理的かどうかである。

$H(a, b, c) = 0$ をその特異点集合の定義 ideal

$$
(6.2)\qquad (H, \frac{\partial H}{\partial a}, \frac{\partial H}{\partial b}, \frac{\partial H}{\partial c}) = (a^2 - 11a - 1, b - 3a - 1, c).
$$

に沿って blow up して非特異化すると、4 度の blow up の後に得られる非特異 model を見ることにより、$\boldsymbol{Q}$ 上で $\mathbf{P}^2$ と双有理同値なことが判る。

定理 2. C_5-固定体 $K^{C_5} = \boldsymbol{Q}(a, b, c)$ は $\boldsymbol{Q}$ 上有理的である。実際、

$$
(6.3)\qquad \begin{cases} A = -\dfrac{2a^3 - 2a^2 + 13a - 7ab + b}{8a^2 - 33a - ab - 7b + 2} \\ B = -\dfrac{c}{8a^2 - 33a - ab - 7b + 2}. \end{cases}
$$

とおけば $K^{C_5} = \boldsymbol{Q}(A,B)$ であり、又、この時、

$$
(6.4) \qquad \begin{cases} a_{\mathrm{num}} := -A^3 - A^2 - 7B^2A + B^2 \\ b_{\mathrm{num}} := 2A^5 - 2A^4 - 8B^2A^4 + 36A^3B^2 - 145B^4A^2 + 3A^2 - 22B^2A^2 \\ \qquad\qquad + 4B^2A + 120B^4A - 2A - 13B^2 - 180B^4 - 625B^6 \\ c_{\mathrm{num}} := -2BP^2 \\ \quad P := A^4 - 2A^3 + 25B^2A^2 - A^2 + 2A + 1 + 25B^2 + 125B^4, \\ \quad Q := -A + 1 + B^2A + 7B^2. \end{cases}
$$

とすれば $a = a_{\mathrm{num}}/Q, b = b_{\mathrm{num}}/Q^2, c = c_{\mathrm{num}}/Q^3$ である。 ▮

<u>系</u>. $f_1^{C_5}(A,B;X) := f^{D_5}(a,b;X)$ は $\boldsymbol{Q}$ 上生成的な C_5-多項式である。又、

$$
(6.5) \qquad f_2^{C_5}(A,B;X) = X^5 - \frac{(2-2A+A^2+15B^2)P}{Q^2}X^3 + \frac{2BP^2}{Q^3}X^2 + \frac{(1-A)P^2}{Q^3}X - \frac{2BP^2}{Q^3},
$$

$$
(6.6) \qquad f_3^{C_5}(A,B;X) = X^5 - \frac{P(A^2+1+10B^2)}{Q^2}X^3 + \frac{(A^2+3B^2+3B^2A^2+25B^4)P^2}{Q^4}X + \frac{2(A^3+A^2+7B^2A-B^2)BP^2}{Q^4},
$$

も $\boldsymbol{Q}$ 上生成的な C_5-多項式である。 ▮

<u>**証明**</u>. 上記の変数変換は $H(a,b,c)=0$ の非特異化の過程で得られる。生成性を示す為、$\mathrm{Gal}(L/K) \simeq C_5$ となる任意の体拡大 $L \supset K \supset \boldsymbol{Q}$ をとる。正規底定理により、$K[C_5]$-加群として $L \simeq K[C_5]$ であり、$L = \bigoplus_{i=1}^{5} Kx_i, \sigma(x_i) = x_{\sigma(i)}$ となる $x_i \in L$ が存在する。(4.3) 等により x, y 及び a, b, c を定めよ。(D_5 の場合と同様に $x = y$ の時は適切に取り直す。) この時、$\mathrm{Gal}(L/K) \simeq C_5$ であることから $c \in K$ となるので、$A, B \in K$ を (6.3) で定めれば、$f_1^{C_5}(A,B;X) \in K[X]$ の K 上の分解体は L に一致する。

$f_2^{C_5}(A,B;X)$ は $x' := x - \alpha(x)$ を根とする多項式として得られる。x' の C_5-軌道を $S' = \mathrm{Orb}_{C_5}(x')$ とし、$f(X) := \prod_{u \in S'}(X-u)$ とすれば、$f(X) \in K^{C_5}$ であり、その K^{C_5} 上の分解体は K である。$f(X)$ の係数を A, B で表して $f_2^{C_5}(A,B;X)$ を得る。x' の代わりに $x'' := x - \alpha^2(x)$ を考えれば、同様にして $f_3^{C_5}(A,B;X)$ を得る。 □

7. Frobenius 群 $F_{5,4}$ (位数 20)

$\alpha=(1\ 2\ 3\ 4\ 5), \gamma=(1\ 5\ 3\ 4) \in \mathfrak{S}_5$ の生成する位数 20 の Frobenius 群 $F_{5,4}=\langle\alpha,\gamma\rangle$ を考える。γ の K への作用は

$$\gamma : \begin{cases} x \longmapsto \dfrac{x}{x-1} \\ y \longmapsto \dfrac{x-1}{x(1-y)} \end{cases} \tag{7.1}$$

となる。$F_{5,4}$ 内での $x \in K$ の固定群は $\langle\gamma^2\rangle$ であるので、$u_0 := x+\gamma(x) = \dfrac{x^2}{x-1}$ は γ-不変で、その $F_{5,4}$-軌道は

$$\begin{aligned} \text{(7.2)} \quad \mathrm{Orb}_{F_{5,4}}(u_0) &= \mathrm{Orb}_{\langle\alpha\rangle}(u_0) \\ &= \left\{ \frac{x^2}{x-1}, -\frac{(1-xy)^2}{xy}, \frac{y^2}{y-1}, -\frac{(1-y)^2}{y(1-x)(1-xy)}, -\frac{(1-x)^2}{x(1-y)(1-xy)} \right\}. \end{aligned}$$

となる。これらを根とする単多項式から、$\boldsymbol{Q}$ 上の生成的 $F_{5,4}$-多項式が得られるが、これは $X \mapsto 1/X$ と変数変換すると次の Lecacheux の多項式 ([Lec]) に一致する。

定理 3 (Lecacheux).

$$\begin{aligned} f^{F_{5,4}}(s,t;X) = X^5 &+ \left(t^2d - 2s - \frac{17}{4}\right)X^4 + \left(3td + d + \frac{13s}{2} + 1\right)X^3 \\ &- \left(td + \frac{11s}{2} - 8\right)X^2 + (s-6)X + 1 \end{aligned}$$

(ここに $d=s^2+4$) は $\boldsymbol{Q}$ 上の生成的 $F_{5,4}$-多項式である。 ∎

8. 交代群 $\mathfrak{A}_5$ (位数 60)

$\alpha=(1\ 2\ 3\ 4\ 5), \omega=(1\ 5\ 4) \in \mathfrak{S}_5$ は交代群 $\mathfrak{A}_5=\langle\alpha,\omega\rangle$ を生成する。ω の K への作用は

$$\omega : \begin{cases} x \longmapsto \dfrac{1}{1-x} \\ y \longmapsto \dfrac{1-x}{1-xy} \end{cases} \tag{8.1}$$

である。$\mathfrak{A}_5$ 内での $x \in K$ の固定群は $\langle(1\ 3)(4\ 5), (1\ 4)(3\ 5)\rangle \simeq V_4$ (Klein の四元群) であるので、$\mathfrak{A}_5$ 内での $v_0 := x+\omega(x)+\omega^2(x) = \dfrac{x^3-3x+1}{x(x-1)}$ の固定群は位数 12 で、その $\mathfrak{A}_5$-軌道は

$$\begin{aligned} \text{(8.2)} \quad \mathrm{Orb}_{\mathfrak{A}_5}(v_0) &= \mathrm{Orb}_{\langle\alpha\rangle}(v_0) \\ &= \left\{ \frac{x^2}{x-1}, -\frac{(1-xy)^2}{xy}, \frac{y^2}{y-1}, -\frac{(1-y)^2}{y(1-x)(1-xy)}, -\frac{(1-x)^2}{x(1-y)(1-xy)} \right\} \end{aligned}$$

である。これらを根とする単多項式から、次の $\boldsymbol{Q}$ 上の生成的 $\mathfrak{A}_5$-多項式を得る。

<u>定理</u> 4. (1) $\mathfrak{A}_5$-固定体 $K^{\mathfrak{A}_5}$ は $\boldsymbol{Q}$ 上有理的である。実際、

$$\text{(8.3)}\qquad \begin{cases} u = \dfrac{a^2 - 10a + 1 - b}{a} \\ v = \dfrac{(2a^5 + 18a^4 - 140a^3 + 13a^2 - 2a) - (4a^3 + 20a^2 + 6a)b - a^2b^2}{a^3} \end{cases}$$

とおけば、$K^{\mathfrak{A}_5} = \boldsymbol{Q}(u, v)$ となる。

(2)

$$\begin{aligned} f^{\mathfrak{A}_5}(u, v; X) = X^5 + uX^4 + (-6u - 10)X^3 + vX^2 \\ + (-u^2 + 12u + 25 - 3v)X + (u^3 + 24u^2 + 27u - 24 + 9v) \end{aligned}$$

は $\boldsymbol{Q}$ 上生成的 $\mathfrak{A}_5$-多項式である。 ∎

<u>注</u>. $f^{\mathfrak{A}_5}$ の判別式は

$$\begin{aligned} ((24000 - 109600u - 54720u^2 + 91032u^3 + 68280u^4 + 13624u^5 + 840u^6 + 16u^7) \\ + (-28400 + 36240u + 44284u^2 + 9240u^3 + 332u^4)v \\ + (6480 + 1386u - 90u^2 - 4u^3)v^2 - 27v^3)^2 \end{aligned}$$

で、既約多項式の平方である。このことは分解体に於ける分岐を統制するのに役立つ。例えば、$a, b \in \boldsymbol{Z}$ に対し判別式が素数の平方 p^2 であれば、p のみで分岐する $\boldsymbol{Q}$ の $\mathfrak{A}_5$-拡大が得られ、p が分岐する 2 次体 K と合成することにより、K 上の不分岐 $\mathfrak{A}_5$-拡大が得られる。

<u>例</u>. $u = -2, v = -1$ とすると、$f^{\mathfrak{A}_5}(-2, -1; X) = X^5 - 2X^4 + 2X^3 - X^2 + 1$ で、判別式は 47^2。

9. 対称群 $\mathfrak{S}_5$ (位数 120)

同様に $\dfrac{(x^2 - x + 1)^3}{x^2(x - 1)^2}$ の $\langle\alpha\rangle$-軌道を根とする単多項式から、$\boldsymbol{Q}$ 上生成的な $\mathfrak{S}_5$-多項式を得ることが出来る (詳細略)。

<u>定理</u> 5. (1) $\mathfrak{S}_5$-固定体 $K^{\mathfrak{S}_5}$ は $\boldsymbol{Q}$ 上有理的。実際、

$$\text{(9.1)}\qquad \begin{cases} U = -u^2 - 15u - 57 \\ V = \dfrac{v + 90}{2u + 15} - 13 \end{cases}$$

とおけば、$K^{\mathfrak{S}_5} = \boldsymbol{Q}(U, V)$ である。

(2)

$$\begin{aligned} f^{\mathfrak{S}_5}(U, V; X) = X^5 + (U - 8)X^4 + (4UV + 3V + 15)X^3 \\ + (4UV^2 + 3V^2 - 4UV - 3V - 2U^2 - 22U - 26)X^2 \\ + (-4U^2V - 15UV - 9V + 3U^2 + 23U + 19)X + U^3 \end{aligned}$$

は $\boldsymbol{Q}$ 上生成的 $\mathfrak{S}_5$-多項式である。 ∎

10. Nöther 問題への応用

以上の結果、特に $K = \boldsymbol{Q}(x,y) = \boldsymbol{Q}(x_1,\ldots,x_5)^{\mathrm{PGL}(2)}$ への 5 次可移群 G の作用の固定体 K^G の有理性の応用として、5 次可移群に対する (本来の) Nöther 問題の直接証明が与えられる。

$L = \boldsymbol{Q}(x_1,\ldots,x_5)$ とし、5 次対称群 $\mathfrak{S}_5$ が変数の置換で作用しているとする。本稿で考えた K への $\mathfrak{S}_5$ の作用はその制限である。$L^{\mathfrak{S}_5}$ は対称式の体であるから $\boldsymbol{Q}$ 上超越次数 5 の純超越拡大であるが、今、これが $K^{\mathfrak{S}_5}$ 上超越次数 3 の純超越拡大であるとせよ。すると $\mathfrak{S}_5$ の部分群 G に対しても、L^G/K^G が超越次数 3 の純超越拡大となる。前節までで全ての 5 次可移群 G に対して K^G が $\boldsymbol{Q}$ 上超越次数 2 の純超越拡大であることを示したので、これより L^G が $\boldsymbol{Q}$ 上超越次数 5 の純超越拡大であることが判る。実際、我々は最近この方法がうまくいくことを示した。

定理 6. $\boldsymbol{Q}(x_1,\ldots,x_5)^{\mathfrak{S}_5}$ は $\boldsymbol{Q}(x,y)^{\mathfrak{S}_5}$ 上有理的である。 ∎

系. 全ての 5 次可移群 G に対して Nöther 問題は肯定的である。即ち、$\boldsymbol{Q}(x_1,\ldots,x_5)^G$ は $\boldsymbol{Q}$ 上有理的である。 ∎

5 次可移群 G に対する Nöther 問題は既に解かれている ([Fu, Ma]) が、特に前田による $\mathfrak{A}_5$ の場合の証明では閉体上での代数幾何の議論を経由しているように思われるので、やや計算に頼る部分もあるが完全に $\boldsymbol{Q}$ 上での議論で具体的に証明できたことには意味があるのではないかと考える。詳細は次の機会に譲る。

参考文献

[Br] A. Brumer, Curves with real multiplications, in preparation.

[BR1] J. Buhler, Z. Reichstein, On the essential dimension of a finite group, Compositio Math. 106 (1997), 159–179.

[BR2] J. Buhler, Z. Reichstein, Versal cyclic polynomials, unpublished manuscript.

[Co] D. F. Coray, Cubic hypersurfaces and a result of Hermite, Duke Math. J. 54-2 (1987), 657–670.

[DM] F. R. DeMeyer, Generic Polynomials, J. Alg. 84 (1983), 441–448.

[Fu] P. Furtwängler, Über Minimalbasen für Körper rationaler Funktionen, S. B. Akad. Wiss. Wien 134 (1925), 69–80.

[Her] C. Hermite, Sur l'invariant du dix-huitième ordre des formes du cinquième degré et sur le role qu'il joue dans la résolution de l'équation de cinquième degré (extrait de deux lettres à M. Borchardt), J. reine angew. Math. 59 (1861), 304–305 (œuvre II, 107–108).

[Has1] K. Hashimoto, On Brumer's family of RM-curves of genus two, Tohoku Math. J. (2) 52 (2000), no. 4, 475–488.

[Has2] K. Hashimoto, Generic families of quintic polynomials with dihedral Galois group of degree 5, 第 45 回代数学シンポジウム報告集 2000 年, 15–23.

[JLY] C. U. Jensen, A.Ledet, N.Yui, Generic Polynomial, contructive aspects of the inverse Galois problem, Mathematical Sciences Reasearch Institute Publications, Cambridge, 2002.

[Lec] O. Lecacheux, Construction de polynômes génériques à groupe de Galois résoluble, Acta Arith. 86 (1998), 207–216.

[Len] H. W. Lenstra, Rational functions invariant under a finite abelian group, Invent. Math. 25 (1974), 299–325.
[Ma] T. Maeda, Noether's problem for A_5, J. Alg. 125 (1989), 418–430.
[Sa] D. J. Saltman, Generic Galois extentions and problems in field theory, Adv. Math. 43 (1982), 250–283.
[Wa] S. Wang, A counterexample to Grunwald's theorem, Ann. of Math. 49(4) (1948), 1008–1009.

早稲田大学理工学部数理科学科 169-8555 東京都新宿区大久保 3–4–1

上智大学理工学部数学科 102-8554 東京都千代田区紀尾井町 7–1
E-mail address: `khasimot@mse.waseda.ac.jp`, `tsuno@mm.sophia.ac.jp`