早稲田大学教育学部　学術研究（数学編）第56号　5～36ページ，2008年2月

生成的多項式の部分体問題に対するチルンハウス変換を用いた幾何学的枠組みについて

星　明考　　三宅　克哉

概　要

任意の基礎体 k に対し，対称群に対する k 上生成的多項式の部分体問題に対処する一般的手法を，チルンハウス変換の定義体を考察することによって与える．前半における一般的考察の結果を基にして，3 次対称群 $\mathfrak{S}_3$，3 次巡回群 C_3 に対する k 上生成的多項式の部分体問題への解を具体的に与える．また，応用として幾つかの 6 次の生成的多項式を具体的に構成する．[1) 2)]

§1. はじめに

任意の標数の体 k を基礎体として固定し，G を有限群とする．基礎体上の m 個の独立変数 $\mathbf{t} = (t_1, \ldots, t_m)$ を取り，$k(\mathbf{t})$ を k 上の m 変数有理関数体とする．多項式 $F(t_1, \ldots, t_m; X) \in k(\mathbf{t})[X]$ は以下の条件 (1),(2) を満たすとき，G に対する k-生成的多項式という：

(1) 多項式 $F(\mathbf{t}; X)$ の $k(\mathbf{t})$ 上のガロア群は G と同型であり，
(2) 各無限体 $M \supset k$ とその G-拡大 L/M に対して，L が $F(\mathbf{a}; X)$ の M 上の最小分解体となるような $\mathbf{a} = (a_1, \ldots, a_m) \in M^m$ が必ず存在する．

さらにこのとき，Kemper の定理 [Kem01] により，任意の部分群 $H \subset G$ に対して，M 上の全ての H-ガロア拡大は (同様にして) $F(\mathbf{t}; X)$ の変数の特殊化 $\mathbf{t} \mapsto \mathbf{a}$ によって得られることが知られている．例えば基本的な [JLY02] には，種々の有限群 G に対する k-生成的多項式が掲載されている．我々は，実際に §6 において幾つかの 6 次生成的多項式を構成する．体 $M \supset k$ 上の任意の H-拡大 ($H \subset G$) は k-生成的多項式の変数の特殊化によって得られる，という事実から次の問題が自然に生じる：

生成的多項式の部分体問題． $F(\mathbf{t}; X)$ を G に対する k-生成的多項式とする．無限体 $M \supset k$ と $\mathbf{a}, \mathbf{b} \in M^m$ に対して，$\mathrm{Spl}_M F(\mathbf{b}; X)$ が $\mathrm{Spl}_M F(\mathbf{a}; X)$ の部分体となるための必要十分条件を与えよ．

1) 本研究の一部は，日本学術振興会科学研究費補助金 基盤研究 (C) 19540057，早稲田大学特定課題研究助成費 2007B-067 の助成を受けている．

2) 本稿のより詳細な内容は，プレプリント "A geometric framework for the subfield problem of generic polynomials via Tschirnhausen transformation" [HM] として Web から入手可能である．

固定した有限群 G に対し，体 M 上の G-ガロア拡大を考察する場合には，次の部分体問題の特別な場合を考えれば十分である：

生成的多項式の同型問題. 無限体 $M \supset k$ と $\mathbf{a}, \mathbf{b} \in M^m$ に対して，$\mathrm{Spl}_M F(\mathbf{a}; X)$ と $\mathrm{Spl}_M F(\mathbf{b}; X)$ が M 上同型となるための必要十分条件を与えよ.

本稿では，n 次対称群 $\mathfrak{S}_n$ に対する k-生成的多項式の同型問題への解法を，チルンハウス変換の定義体を通じて考察する．まず§2, §3 において一般の対称群 $\mathfrak{S}_n$ に対する検討を行い，その結果を基にして，§4, §5 で $\mathfrak{S}_3, C_3$ に対する k-生成的多項式の部分体問題への解を与える.

体 K 上の代数閉体を固定し，K 上の分離的でモニックな n 次多項式 $f(X) \in K[X]$ に対し，$\alpha_1, \ldots, \alpha_n$ を $f(X)$ のその中での根とする．次の形の多項式 $g(X) \in K[X]$ を $f(X)$ の体 K 上のチルンハウス変換という：

$$g(X) = \prod_{i=1}^{n} \bigl(X - (c_0 + c_1\alpha_i + \cdots + c_{n-1}\alpha_i^{n-1})\bigr), \quad c_i \in K.$$

多項式 $f(X), g(X) \in K[X]$ が互いに K 上のチルンハウス変換で移り合うとき，多項式 $f(X)$ と $g(X)$ は K 上チルンハウス同値であるという．既約分離的多項式 $f(X), g(X) \in K[X]$ に対して，次は同値である：

(i) $f(X)$ と $g(X)$ は K 上チルンハウス同値である；
(ii) 商体 $K[X]/(f(X))$ と $K[X]/(g(X))$ は K 上同型である.

§2. チルンハウス変換 (幾何学的な解釈)

まず $n \geq 3$ を正整数とし，$\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ を k 上の $2n$ 個の独立変数とする．さらに $f_n(\mathbf{s}; X) = f_n(s_1, \ldots, s_n; X) \in k(\mathbf{s})[X]$, $f_n(\mathbf{t}; X) = f_n(t_1, \ldots, t_n; X) \in k(\mathbf{t})[X]$ をモニックな n 次多項式とし，それらの根がそれぞれ $\{x_1, \ldots, x_n\}, \{y_1, \ldots, y_n\}$ であるとすれば

$$f_n(\mathbf{s}; X) = \prod_{i=1}^{n}(X - x_i) = X^n - s_1X^{n-1} + s_2X^{n-2} + \cdots + (-1)^n s_n,$$
$$f_n(\mathbf{t}; X) = \prod_{i=1}^{n}(X - y_i) = X^n - t_1X^{n-1} + t_2X^{n-2} + \cdots + (-1)^n t_n$$

が得られる．但し，s_i, t_i はそれぞれ $x_1, \ldots, x_n$ 及び $y_1, \ldots, y_n$ に対する i 次基本対称式である．体 K を

$$K := k(\mathbf{s}, \mathbf{t})$$

によって定めれば，K は自然に k 上の $2n$ 変数有理関数体と見なせる．また，

$$L_{\mathbf{s}} := \mathrm{Spl}_K f_n(\mathbf{s}; X) = K(x_1, \ldots, x_n),$$

$$L_{\mathbf{t}} := \mathrm{Spl}_K f_n(\mathbf{t}; X) = K(y_1, \ldots, y_n)$$

とおけば，$L_{\mathbf{s}} \cap L_{\mathbf{t}} = K$ かつ $L_{\mathbf{s}}L_{\mathbf{t}} = k(\mathbf{x}, \mathbf{y})$ である．したがって，体の拡大 $k(\mathbf{x}, \mathbf{y})/K$ はガロア拡大であり，そのガロア群は n 次対称群 $\mathfrak{S}_n$ の 2 つの直積 $\mathfrak{S}_n \times \mathfrak{S}_n$ と同型になる．ここで

$$G_{\mathbf{s}} := \mathrm{Gal}(L_{\mathbf{s}}L_{\mathbf{t}}/L_{\mathbf{t}}), \quad G_{\mathbf{t}} := \mathrm{Gal}(L_{\mathbf{s}}L_{\mathbf{t}}/L_{\mathbf{s}})$$

かつ

$$G_{\mathbf{s},\mathbf{t}} := G_{\mathbf{s}} \times G_{\mathbf{t}}$$

と置く．群 $G_{\mathbf{s},\mathbf{t}} \cong \mathrm{Gal}(L_{\mathbf{s}}L_{\mathbf{t}}/K)$ は $k(\mathbf{x}, \mathbf{y})$ に右から作用するとする．そこで，$g = (\sigma, \tau) \in G_{\mathbf{s},\mathbf{t}}$ に対して，逆同型

$$\varphi : G_{\mathbf{s}} \to \mathfrak{S}_n, \quad \sigma \mapsto \varphi(\sigma),$$
$$\psi : G_{\mathbf{t}} \to \mathfrak{S}_n, \quad \tau \mapsto \psi(\tau),$$

を固定し，群 $G_{\mathbf{s},\mathbf{t}}$ と $\mathfrak{S}_n \times \mathfrak{S}_n$ を以下の作用で同一視する：

$$x_i^{\sigma} = x_{\varphi(\sigma)(i)}, \quad y_i^{\sigma} = y_i, \quad x_i^{\tau} = x_i, \quad y_i^{\tau} = y_{\psi(\tau)(i)}, \quad (i = 1, \ldots, n). \tag{1}$$

さて $f_n(\mathbf{s}; X)$ から $f_n(\mathbf{t}; X)$ へのチルンハウス変換は，K の代数閉体の中では $n!$ 個存在する．我々はまず，$f_n(\mathbf{s}; X)$ から $f_n(\mathbf{t}; X)$ へのチルンハウス変換の定義体 (K の拡大体) を考察する．行列 D を

$$D := \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

と定義する (Vandermonde 行列)．行列 D の行列式は

$$\det D = \Delta_{\mathbf{s}}, \quad \text{但し} \quad \Delta_{\mathbf{s}} := \prod_{1 \le i < j \le n} (x_j - x_i)$$

によって与えられ，D は可逆である．体 $k(\mathbf{s})(\Delta_{\mathbf{s}})$ は $\mathrm{char}\ k \neq 2$，すなわち体 k の標数が 2 でないならば，$k(\mathbf{s})$ の 2 次拡大を与えていることに注意しよう．体 $k(\mathbf{x}, \mathbf{y})$ の中で n 個の元の組 $(u_0(\mathbf{x}, \mathbf{y}), \ldots, u_{n-1}(\mathbf{x}, \mathbf{y})) \in k[\mathbf{x}, \mathbf{y}, \Delta_{\mathbf{s}}^{-1}]^n$ を以下のように定義する：

$$\begin{pmatrix} u_0(\mathbf{x}, \mathbf{y}) \\ u_1(\mathbf{x}, \mathbf{y}) \\ \vdots \\ u_{n-1}(\mathbf{x}, \mathbf{y}) \end{pmatrix} := D^{-1} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}. \tag{2}$$

クラメールの公式から

$$u_i(\mathbf{x},\mathbf{y}) = \Delta_{\mathbf{s}}^{-1}\cdot\det\begin{pmatrix} 1 & x_1 & \cdots & x_1^{i-1} & y_1 & x_1^{i+1} & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{i-1} & y_2 & x_2^{i+1} & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{i-1} & y_n & x_n^{i+1} & \cdots & x_n^{n-1} \end{pmatrix} \tag{3}$$

を得る．また，表記を簡略にするために

$$u_i := u_i(\mathbf{x},\mathbf{y}),\quad (i=0,\ldots,n-1)$$

と書くことにする．ガロア群 $G_{\mathbf{s},\mathbf{t}}$ は軌道 $\{u_i^{(\sigma,\tau)} \mid (\sigma,\tau)\in G_{\mathbf{s},\mathbf{t}}\}$ に右から作用するが，この作用は忠実ではない．ここで，部分群 $H\subset G_{\mathbf{s},\mathbf{t}}$ を

$$H := \{(\sigma,\tau)\in G_{\mathbf{s},\mathbf{t}} \mid \varphi(\sigma)=\psi(\tau)\}\cong \mathfrak{S}_n$$

によって定め，$\overline{g}=Hg$ を H の $G_{\mathbf{s},\mathbf{t}}$ における右剰余類とする．このとき $(\sigma,\tau)\in H$ に対して $u_i^{(\sigma,\tau)}=u_i, (i=0,\ldots,n-1)$ であることが下の補題から分かる．これより，群 $G_{\mathbf{s},\mathbf{t}}$ は集合 $\{u_i^g \mid \overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}\}$ に右剰余類からなる集合 $H\backslash G_{\mathbf{s},\mathbf{t}}$ への作用を通して作用する．また，集合 $\{\overline{(1,\tau)} \mid (1,\tau)\in G_{\mathbf{s},\mathbf{t}}\}$ 及び $\{\overline{(\sigma,1)} \mid (\sigma,1)\in G_{\mathbf{s},\mathbf{t}}\}$ は $H\backslash G_{\mathbf{s},\mathbf{t}}$ の完全代表系である．実際，たとえば $g=(\sigma,\tau)\in G_{\mathbf{s},\mathbf{t}}$ に対して $\varphi(\sigma)=\psi(\tau')$ とすれば $\overline{g}=H(\sigma,\tau')^{-1}g=H(1,(\tau')^{-1}\tau)$ が成り立つ．

補題 2.1.　整数 i, $(0\le i\le n-1)$, を固定する．もし $(\sigma,\tau)\in G_{\mathbf{s},\mathbf{t}}$ に対し $u_i^{(\sigma,\tau)}=u_i$ であるならば，$\varphi(\sigma)=\psi(\tau)$ であり，またその逆も成り立つ．すなわち，$H=\mathrm{Stab}_{G_{s,t}}(u_i)$ である．

証明.　[HM] 参照.　□

この補題から，特に $\#H\backslash G_{\mathbf{s},\mathbf{t}}=n!$ であり，$G_{\mathbf{s},\mathbf{t}}$ の部分群 $G_{\mathbf{s}}$ 及び $G_{\mathbf{t}}$ は集合 $\{u_i^g \mid \overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}\}$ に忠実に作用する．特に $\overline{g}=\overline{(1,\tau)}$ に対して，定義 (2) より次の等式が得られる：

$$y_{\psi(\tau)(i)} = u_0^g + u_1^g x_i + \cdots + u_{n-1}^g x_i^{n-1},\quad (i=1,\ldots,n).$$

これは各 $\overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}$ に対して，集合 $\{(u_0^g,\ldots,u_{n-1}^g) \mid \overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}\}$ が $f_n(\mathbf{s};X)$ から $f_n(\mathbf{t};X)$ へのチルンハウス変換の係数を与えることを意味している．

定義.　各 $\overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}$ に対して，体 $K(u_0^g,\ldots,u_{n-1}^g)$ を $f_n(\mathbf{s};X)$ から $f_n(\mathbf{t};X)$ へのチルンハウス変換の係数の体と呼ぶ．

また $u_i(\mathbf{x},\mathbf{y})$ の $\mathbf{x}$ と $\mathbf{y}$ を入れ換えて

$$v_i(\mathbf{x},\mathbf{y}) := u_i(\mathbf{y},\mathbf{x}),\quad (i=0,\ldots,n-1)$$

と置き，簡単の為に $v_i=v_i(\mathbf{x},\mathbf{y})$ と書くことにする．体 $K(v_0^g,\ldots,v_{n-1}^g)$ は $f_n(\mathbf{t};X)$ から $f_n(\mathbf{s};X)$ へのチルンハウス変換の係数の体を与える．

命題 2.2.　各整数 $i, (0 \leq i \leq n-1)$, 及び $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$(L_{\mathbf{s}}L_{\mathbf{t}})^{g^{-1}Hg} = K(u_0^g, \ldots, u_{n-1}^g) = K(v_0^g, \ldots, v_{n-1}^g) = K(u_i^g) = K(v_i^g)$ であり，かつ $[K(u_i^g) : K] = n!$ が成り立つ．

証明.　$\mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(u_i^g) = \mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(v_i^g) = g^{-1}Hg$ から直接従う ([HM] 参照)．　□

系 2.3.　各 $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$\mathrm{Spl}_{K(u_i^g)} f_n(\mathbf{s}; X) = \mathrm{Spl}_{K(u_i^g)} f_n(\mathbf{t}; X)$ である．

証明.　多項式 $f_n(\mathbf{s}; X)$ と $f_n(\mathbf{t}; X)$ は体 $K(u_0^g, \ldots, u_{n-1}^g) = K(u_i^g) = K(v_i^g)$ の上でチルンハウス同値である．よって，商体 $K(u_i^g)[X]/(f_n(\mathbf{s}; X))$ と $K(u_i^g)[X]/(f_n(\mathbf{t}; X))$ は $K(u_i^g)$ 上同型である．　□

命題 2.4.　次が成り立つ．

(i) $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$L_{\mathbf{s}} \cap K(u_i^g) = L_t \cap K(u_i^g) = K$ であり，
(ii) $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$L_{\mathbf{s}}L_{\mathbf{t}} = L_{\mathbf{s}}(u_i^g) = L_{\mathbf{t}}(u_i^g)$ である．

証明.　(i) は $(g^{-1}Hg)G_{\mathbf{t}} = (g^{-1}Hg)G_{\mathbf{s}} = G_{\mathbf{s},\mathbf{t}}$ を，(ii) は $g^{-1}Hg \cap G_{\mathbf{s}} = g^{-1}Hg \cap G_{\mathbf{t}} = \{1\}$ を示せばよい ([HM] 参照)．　□

さらに，次の命題が得られる．

命題 2.5.　各整数 $i, (0 \leq i \leq n-1)$, に対して，$L_{\mathbf{s}}L_{\mathbf{t}} = K(u_i^g \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}})$ が成り立つ．

証明.　$\mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(u_i^g) = g^{-1}Hg$ であるから，$\bigcap_{\overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}} g^{-1}Hg = \{1\}$ を示せばよい ([HM] 参照)．　□

ここで，次数 $n!$ の多項式を以下のように定義する：

$$F_i(\mathbf{s}, \mathbf{t}; X) := \prod_{\overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}} (X - u_i^g) \in K[X], \quad (i = 0, \ldots, n-1).$$

命題 2.2 より $F_i(\mathbf{s}, \mathbf{t}; X), (i = 0, \ldots, n-1)$, は $k(\mathbf{s}, \mathbf{t})$ 上既約である．さらに，命題 2.5 から次の定理が得られる．

定理 2.6.　多項式 $F_i(\mathbf{s}, \mathbf{t}; X) \in k(\mathbf{s}, \mathbf{t})[X]$ は $\mathfrak{S}_n \times \mathfrak{S}_n$ に対して k-生成的である．

証明.　定理の主張は，$\mathrm{Spl}_K F_i(\mathbf{s}, \mathbf{t}; X) = K(u_i^g \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}) = L_{\mathbf{s}}L_{\mathbf{t}}$ であること，および，$f_n(\mathbf{s}; X)$ と $f_n(\mathbf{t}; X)$ がそれぞれ $\mathfrak{S}_n$ に対する k-生成的多項式であることから従う．　□

体 k の標数が 2 である場合には，$\Delta_{\mathbf{s}} \in k(\mathbf{s})$ となり，$k(\mathbf{s})(\Delta_{\mathbf{s}}) = k(\mathbf{s})$ である．よって，$k(\mathbf{s})(\Delta_{\mathbf{s}})$ は $k(\mathbf{s})$ の 2 次拡大体にはならない．そこで標数が 2 の場合には，Berlekamp [Ber76] に従って Berlekamp の判別式と呼ばれる

$$\beta_{\mathbf{s}} := \sum_{i<j} \frac{x_i}{x_i + x_j}$$

を通常の差積 $\Delta_{\mathbf{s}}$ の代わりに用いる．このとき，$k(\mathbf{s})(\beta_{\mathbf{s}})$ は $k(\mathbf{s})$ の 2 次拡大体となる．

次数 n の交代群 $\mathfrak{A}_n$ に対して，

$$(H\backslash G_{\mathbf{s},\mathbf{t}})^+ := \{\overline{g} = \overline{(1,\tau)} \in H\backslash G_{\mathbf{s},\mathbf{t}} \mid \psi(\tau) \in \mathfrak{A}_n\},$$
$$(H\backslash G_{\mathbf{s},\mathbf{t}})^- := \{\overline{g} = \overline{(1,\tau)} \in H\backslash G_{\mathbf{s},\mathbf{t}} \mid \psi(\tau) \notin \mathfrak{A}_n\}$$

とおき，多項式 $F_i^+(X), F_i^-(X)$ を以下の様に定義する．

$$F_i^{\pm}(X) := \prod_{\overline{g}\in(H\backslash G_{\mathbf{s},\mathbf{t}})^{\pm}} (X - u_i^g), \quad (i = 0,\ldots,n-1). \tag{4}$$

命題 2.7. 多項式 $F_i(\mathbf{s},\mathbf{t};X)$ は K の 2 次拡大体 $K(\Delta_{\mathbf{s}}/\Delta_{\mathbf{t}})$ 上で (char $k = 2$ の場合は，$K(\beta_{\mathbf{s}}+\beta_{\mathbf{t}})$ 上で)，2 つの $n!/2$ 次既約多項式 $F_i^+(X)$, $F_i^-(X)$ の積となる．

証明. [HM] 参照. □

§3. 無限体への変数の特殊化

さて M ($\supset k$) を無限体とする．ここで考察する多項式 $f_n(\mathbf{s};X)$, $f_n(\mathbf{t};X)$ の変数の特殊化 $(\mathbf{s},\mathbf{t}) \mapsto (\mathbf{a},\mathbf{b}) \in M^n \times M^n$ については，$f_n(\mathbf{a};X)$, $f_n(\mathbf{b};X)$ は M 上分離的であると仮定することにする (すなわち $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$)．多項式 $f_n(\mathbf{a};X)$, $f_n(\mathbf{b};X)$ の M の固定された代数閉包の中での最小分解体を $L_{\mathbf{a}} = \mathrm{Spl}_M f_n(\mathbf{a};X)$, $L_{\mathbf{b}} = \mathrm{Spl}_M f_n(\mathbf{b};X)$ とおく．また $f_n(\mathbf{a};X)$, $f_n(\mathbf{b};X)$ の M 上のガロア群をそれぞれ $G_{\mathbf{a}}, G_{\mathbf{b}}$ とする，(すなわち，$G_{\mathbf{a}} = \mathrm{Gal}(L_{\mathbf{a}}/M)$, $G_{\mathbf{b}} = \mathrm{Gal}(L_{\mathbf{b}}/M)$)．さらに，$G_{\mathbf{a},\mathbf{b}} := \mathrm{Gal}(L_{\mathbf{a}}L_{\mathbf{b}}/M)$ とおく．固定しておいた M の代数閉包の中で，$f_n(\mathbf{a};X)$, $f_n(\mathbf{b};X)$ それぞれの根 $\boldsymbol{\alpha} := (\alpha_1,\ldots,\alpha_n)$, $\boldsymbol{\beta} := (\beta_1,\ldots,\beta_n)$ をとる．根の順序を固定することによって，ガロア群 $G_{\mathbf{a},\mathbf{b}}$ の各要素は，2 つの添え字集合の置換を引き起こす．よって，$G_{\mathbf{a},\mathbf{b}}$ は $G_{\mathbf{s},\mathbf{t}}$ の部分群と見なすことができる．より正確に言えば，要素 $h \in G_{\mathbf{a},\mathbf{b}}$ が $\alpha_i^h = \alpha_{\varphi(\sigma)(i)}$, $\beta_i^h = \beta_{\psi(\tau)(i)}$, $(i = 1,\ldots,n)$, を満たすとき，$h = (\sigma,\tau) \in G_{\mathbf{s},\mathbf{t}}$ と書くことにする．ここで $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$ が基本的にきいている．

各 $g = (\sigma,\tau) \in G_{\mathbf{s},\mathbf{t}}$ に対して，次のようにおく：

$$(c_0^g,\ldots,c_{n-1}^g) := (u_0^g(\boldsymbol{\alpha},\boldsymbol{\beta}),\ldots,u_{n-1}^g(\boldsymbol{\alpha},\boldsymbol{\beta})), \tag{5}$$
$$(d_0^g,\ldots,d_{n-1}^g) := (u_0^g(\boldsymbol{\beta},\boldsymbol{\alpha}),\ldots,u_{n-1}^g(\boldsymbol{\beta},\boldsymbol{\alpha})).$$

定義から，$i = 1,\ldots,n$ に対して

$$\beta_{\psi(\tau)(i)} = c_0^g + c_1^g\alpha_{\varphi(\sigma)(i)} + \cdots + c_{n-1}^g\alpha_{\varphi(\sigma)(i)}^{n-1}, \tag{6}$$
$$\alpha_{\varphi(\sigma)(i)} = d_0^g + d_1^g\beta_{\psi(\tau)(i)} + \cdots + d_{n-1}^g\beta_{\psi(\tau)(i)}^{n-1} \tag{7}$$

が成り立つ．したがって，各 $\overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}$ に対して，$f_n(\mathbf{a};X)$ から $f_n(\mathbf{b};X)$ への $M(c_0^g,\ldots,c_{n-1}^g)$ 上のチルンハウス変換が存在する．また $(c_0^g,\ldots,c_{n-1}^g)$ に対して，$(d_0^g,\ldots,d_{n-1}^g)$ はその逆変換のチルンハウス変換の係数を与える．

仮定 $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$ より，次の補題が得られる．

補題 3.1. 体の拡大 M'/M に対して，もし $f_n(\mathbf{b};X)$ が M' 上において $f_n(\mathbf{a};X)$ のチルンハウス変換であるならば，$f_n(\mathbf{a};X)$ は $f_n(\mathbf{b};X)$ の M' 上でのチルンハウス変換である．特に，各 $g \in G_{\mathbf{s},\mathbf{t}}$ に対して $M(c_0^g,\ldots,c_{n-1}^g) = M(d_0^g,\ldots,d_{n-1}^g)$ が成り立つ．

証明. [HM] 参照. □

本稿の主題の一つは，$f_n(\mathbf{a};X)$ から $f_n(\mathbf{b};X)$ へのチルンハウス変換の係数の体 $M(c_0^g,\ldots,c_{n-1}^g)$ の振る舞いを考察することである．

命題 3.2. 仮定 $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$ の下で，次が成立する：

(i) $g \in G_{\mathbf{s},\mathbf{t}}$ に対し，$\mathrm{Spl}_{M(c_0^g,\ldots,c_{n-1}^g)} f_n(\mathbf{a};X) = \mathrm{Spl}_{M(c_0^g,\ldots,c_{n-1}^g)} f_n(\mathbf{b};X)$;
(ii) $g \in G_{\mathbf{s},\mathbf{t}}$ に対し，$L_{\mathbf{a}} L_{\mathbf{b}} = L_{\mathbf{a}}\, M(c_0^g,\ldots,c_{n-1}^g) = L_{\mathbf{b}}\, M(c_0^g,\ldots,c_{n-1}^g)$.

証明. 補題 3.1 より，$M' = M(c_0^g,\ldots,c_{n-1}^g)$ に対して $M'[X]/(f_n(\mathbf{a};X))$ と $M'[X]/(f_n(\mathbf{b};X))$ は M' 上同型である．よって (i) が従う．また (i) より，$L_{\mathbf{a}}\, M(c_0^g,\ldots,c_{n-1}^g) = L_{\mathbf{b}} M(c_0^g,\ldots,c_{n-1}^g)$ であり，(ii) が従う. □

命題 2.2 と命題 2.5 から，$j, (0 \leq j \leq n-1)$, を固定したとき，次が成り立つ：

$$K(u_0^g,\ldots,u_{n-1}^g) \;=\; K(u_j^g), \quad (g \in G_{\mathbf{s},\mathbf{t}}), \tag{8}$$

$$L_{\mathbf{s}} L_{\mathbf{t}} \;=\; K(u_j^g \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}) \tag{9}$$

かつ $[K(u_j^g) : K] = n!$. しかしながら，式 (5) における特殊化の後，一般に成り立つのは包含関係

$$M(c_0^g,\ldots,c_{n-1}^g) \;\supset\; M(c_j^g), \quad (g \in G_{\mathbf{s},\mathbf{t}}),$$

$$L_{\mathbf{a}} L_{\mathbf{b}} \;\supset\; M(c_j^g \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}})$$

のみであり，$M(c_0^g,\ldots,c_{n-1}^g) = M(c_j^g)$ が成り立つかどうかは，特殊化 $(\mathbf{s},\mathbf{t}) \mapsto (\mathbf{a},\mathbf{b}) \in M^n \times M^n$ に依存して決まる．

式 (8) から，次のような多項式 $P_{i,j}(\mathbf{s},\mathbf{t};X) \in K[X]$ が存在する事が分かる：

$$u_i = P_{i,j}(\mathbf{s},\mathbf{t};u_j) \quad \text{かつ} \quad \deg_X(P_{i,j}(\mathbf{s},\mathbf{t};X)) < n!.$$

よって $P_{i,j}(\mathbf{s},\mathbf{t};X)$ の X に関する各係数の分母を (重複を除いて) 取り出せば，

$$u_i = \frac{1}{D^0_{i,j}(\mathbf{s},\mathbf{t})} P^0_{i,j}(\mathbf{s},\mathbf{t};u_j) \quad \text{かつ} \quad \deg_X(P^0_{i,j}(\mathbf{s},\mathbf{t};X)) < n! \tag{10}$$

を満たすような多項式 $P^0_{i,j}(\mathbf{s},\mathbf{t};X) \in k[\mathbf{s},\mathbf{t}][X]$ と $D^0_{i,j}(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ が得られる．

補題 3.3. ある $j, (0 \leq j \leq n-1)$, と $\mathbf{a}, \mathbf{b} \in M^n$ に対し，もし各 $i = 0, \ldots, n-1$, に対して $D^0_{i,j}(\mathbf{a}, \mathbf{b}) \neq 0$ であるならば，各 $g \in G_{\mathbf{s},\mathbf{t}}$ に対して $M(c_0^g, \ldots, c_{n-1}^g) = M(c_j^g)$ が成り立つ．

式 (5) による特殊化後に対しても，次数 $n!$ の多項式

$$F_i(\mathbf{a}, \mathbf{b}; X) = \prod_{\overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}} (X - c_i^g) \in M[X], \quad (i = 0, \ldots, n-1)$$

を用いる．ただし $F_i(\mathbf{a}, \mathbf{b}; X)$ は M 上既約であるとは限らない．

補題 3.4. ある $j, (0 \leq j \leq n-1)$, に対し，$F_j(\mathbf{a}, \mathbf{b}; X)$ は M 上既約であるとする．このとき，$i = 0, \ldots, n-1$, に対して $D^0_{i,j}(\mathbf{a}, \mathbf{b}) \neq 0$ である．

証明. 実際，ある i に対して $D^0_{i,j}(\mathbf{a}, \mathbf{b}) = 0$ であると仮定すれば $P^0_{i,j}(\mathbf{a}, \mathbf{b}; c_j) = 0$ でなくてはならない．ところが $P^0_{i,j}(\mathbf{a}, \mathbf{b}; X) \in k[\mathbf{a}, \mathbf{b}][X]$ の次数は $n!$ 未満であり，これはやはり c_j を根に持つ次数 $n!$ の多項式 $F_j(\mathbf{a}, \mathbf{b}; X) \in k[\mathbf{a}, \mathbf{b}][X]$ が M 上既約であることに矛盾する． □

命題 3.5. ある $j, (0 \leq j \leq n-1)$, と $\mathbf{a}, \mathbf{b} \in M^n$, $(\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0)$, に対して，もし各 $i = 0, \ldots, n-1$, について $D^0_{i,j}(\mathbf{a}, \mathbf{b}) \neq 0$ であるならば，$F_j(\mathbf{a}, \mathbf{b}; X)$ は重根を持たない．

証明. [HM] 参照． □

更に分析を進める前に，ここで集合 $\{c_i^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$, $(0 \leq i \leq n-1)$ への群 $G_{\mathbf{s},\mathbf{t}}$ と群 $G_{\mathbf{a},\mathbf{b}}$ の作用について考察しておく．ここで $g \in G_{\mathbf{s},\mathbf{t}}$ は右剰余類の集合 $H \backslash G_{\mathbf{s},\mathbf{t}}$ の完全代表系を動き，c_i^g は $c_i^g = u_i^g(\boldsymbol{\alpha}, \boldsymbol{\beta})$ によって定義されたのであった．独立な $2n$ 変数 $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ の有理関数 $u_i(\mathbf{x}, \mathbf{y})$ は体 $L_{\mathbf{s}} L_{\mathbf{t}} = k(\mathbf{x}, \mathbf{y})$ に属し，ガロア群 $G_{\mathbf{s},\mathbf{t}} = \mathrm{Gal}(L_{\mathbf{s}} L_{\mathbf{t}} / k(\mathbf{s}, \mathbf{t}))$ は集合 $\{x_1, \ldots, x_n\}$ と $\{y_1, \ldots, y_n\}$ への置換を通して，自然に $u_i(\mathbf{x}, \mathbf{y})$ たちに作用する： $g = (\sigma, \tau) \in G_{\mathbf{s},\mathbf{t}}$ に対し，$u_i^g(\mathbf{x}, \mathbf{y}) = u_i(\mathbf{x}^g, \mathbf{y}^g)$, $\mathbf{x}^g = (x_{\varphi(\sigma)(1)}, \ldots, x_{\varphi(\sigma)(n)})$, $\mathbf{y}^g = (y_{\psi(\tau)(1)}, \ldots, x_{\psi(\tau)(n)})$.

しかしながら，群 $G_{\mathbf{s},\mathbf{t}}$ はガロア群として直接 u_i^g の値の集合 $\{c_i^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ に作用しているわけではない．数値 c_i^g は右剰余類 Hg の値だけで決まることから，c_i^g, $(\overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}})$, を，$H \backslash G_{\mathbf{s},\mathbf{t}}$ 上定義された関数 $\mathbf{c}_i(g) := c_i^g$ とみなす．このとき，$h \in G_{\mathbf{s},\mathbf{t}}$ に対し，$\mathbf{c}_i^h(g) := c_i^{gh}$ は $H \backslash G_{\mathbf{s},\mathbf{t}}$ 上の h による平行移動と関数 $\mathbf{c}_i$ との合成として捉えられ，各 $h \in G_{\mathbf{s},\mathbf{t}}$ は値の集合 $\{c_i^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ の置換を引き起こす．この様にして，$G_{\mathbf{s},\mathbf{t}}$ は $\{c_i^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ に可移的に作用している．もし $\#\{c_i^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\} = n!$ であれば，$\#(H \backslash G_{\mathbf{s},\mathbf{t}}) = n!$ であるから $\mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(c_i^g) = \mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(u_i^g(\mathbf{x}, \mathbf{y})) = g^{-1} H g$ が成り立つ．

ガロア群 $G_{\mathbf{a},\mathbf{b}}$ に対しては，状況は異なる．各 c_i^g は体 $L_{\mathbf{a}} L_{\mathbf{b}}$ に含まれているので，$G_{\mathbf{a},\mathbf{b}}$ は集合 $\{c_i^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ に対して直接にガロア群 $\mathrm{Gal}(L_{\mathbf{a}} L_{\mathbf{b}} / M)$ として作用する．さらに，仮定 $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$ の下で，$G_{\mathbf{a},\mathbf{b}}$ は $G_{\mathbf{s},\mathbf{t}}$ の部分群と見なすことができた．

補題 3.6. 群 $G_{\mathbf{a},\mathbf{b}}$ の集合 $\{c_i^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ へのガロア群 $\mathrm{Gal}(L_{\mathbf{a}} L_{\mathbf{b}} / M)$ としての作用と，$G_{\mathbf{s},\mathbf{t}}$ の部分群としての $G_{\mathbf{s},\mathbf{t}}$ の $H \backslash G_{\mathbf{s},\mathbf{t}}$ への作用から得られる作用とは一致する．

証明. [HM] 参照. □

命題 3.7. 通例のように $\mathbf{a}, \mathbf{b} \in M^n$ に対して $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$ を仮定する．さらに，ある $j, (0 \leq j \leq n-1)$, に対して多項式 $F_j(\mathbf{a}, \mathbf{b}; X)$ は重根を持たないとする．このとき，次が成り立つ：
(i) 各 $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$M(c_0^g, \ldots, c_{n-1}^g) = M(c_j^g)$;
(ii) $L_{\mathbf{a}} L_{\mathbf{b}} = M(c_j^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}})$.

証明. [HM] 参照. □

定理 3.8. ある $j, (0 \leq j \leq n-1)$, と $\mathbf{a}, \mathbf{b} \in M^n$, $(\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0)$, に対して，多項式 $F_j(\mathbf{a}, \mathbf{b}; X)$ は重根を持たないとする．このとき，剰余環 $M[X]/(f_n(\mathbf{a}; X))$ と $M[X]/(f_n(\mathbf{b}; X))$ が M 上同型となるためには，$F_j(\mathbf{a}, \mathbf{b}; X)$ が M 内に根を持つことが必要十分である．

証明. [HM] 参照. □

群 $G_{\mathbf{a}}$ と群 $G_{\mathbf{b}}$ が同じ群 G と同型であり，G の指数 n の全ての部分群は G-共役であるとき，$F_j(\mathbf{a}, \mathbf{b}; X)$ を用いて生成的多項式の同型問題に解を与えることができる．

系 3.9. 整数 j と $\mathbf{a}, \mathbf{b} \in M^n$ を定理 3.8 と同様とする．また $G_{\mathbf{a}}$ と $G_{\mathbf{b}}$ はある群 G に同型であって，G の指数 n の全ての部分群は G-共役であると仮定する．このとき，$\mathrm{Spl}_M(f_n(\mathbf{a}; X))$ と $\mathrm{Spl}_M(f_n(\mathbf{b}; X))$ が一致するためには，$F_j(\mathbf{a}, \mathbf{b}; X)$ が M 内に根を持つことが必要十分である．

もし群 G が，n 次対称群 $\mathfrak{S}_n$, $(n \neq 6)$, n 次交代群 $\mathfrak{A}_n$, $(n \neq 6)$, または，ある素数 p に対する，p 次対称群 $\mathfrak{S}_p$ の可解な可移部分群であるとすると，指数 n (最後の場合には p) の全ての部分群は G-共役となる ([Hup67], [BJY86] 参照).

さて H_1, H_2 を $\mathfrak{S}_n$ の部分群とする．定理 2.6 の類似として，直積 $H_1 \times H_2$ に対する k-生成的多項式が次のようにして得られる．

定理 3.10. 基礎体 k 上の $(k+l)$ 変数有理関数体を $M = k(q_1, \ldots, q_k, r_1, \ldots, r_l)$, $(1 \leq k, l \leq n-1)$ とし，$\mathbf{a} \in k(q_1, \ldots, q_k)^n$, $\mathbf{b} \in k(r_1, \ldots, r_l)^n$ に対して，$f_n(\mathbf{a}; X) \in M[X]$ と $f_n(\mathbf{b}; X) \in M[X]$ はそれぞれ H_1 と H_2 に対する k-生成的多項式であるとする．さらに，ある $j, (0 \leq j \leq n-1)$, に対し，$F_j(\mathbf{a}, \mathbf{b}; X) \in M[X]$ は重根を持たないとする．このとき，$F_j(\mathbf{a}, \mathbf{b}; X)$ は $H_1 \times H_2$ に対する k-生成的多項式である．但し，$F_j(\mathbf{a}, \mathbf{b}; X)$ は M 上既約であるとは限らない．

証明. 命題 3.7 より $M(c_j^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}) = L_{\mathbf{a}} L_{\mathbf{b}}$ が従う．よって定理の主張は $f_n(\mathbf{a}; X)$ の H_1-生成性と $f_n(\mathbf{b}; X)$ の H_2-生成性から従う. □

チルンハウス同値の各同値類に対し，$a_1 = 0$ かつ $a_{n-1} = a_n$ を満たす多項式 $f_n(\mathbf{s}; X)$ が存在することが知られている．すなわち，$a_1 = 0$ かつ $a_{n-1} = a_n$ である特殊化 $\mathbf{s} \mapsto \mathbf{a} \in M^n$ が常に選べる ([JLY02, §8.2] 参照)．よって多項式

$$
\begin{aligned}
&g_n(q_2,\ldots,q_{n-1};X)\\
&:=(-1)^n\cdot f_n(0,q_2,\ldots,q_{n-2},q_{n-1},q_{n-1};-X)\\
&=X^n+q_2X^{n-2}+\cdots+q_{n-2}X^2+q_{n-1}X+q_{n-1}
\end{aligned}
$$

は任意の基礎体 k に対し，$\mathfrak{S}_n$ に対する $(n-2)$ パラメータ $q_2,\ldots,q_{n-1}$ 付きの k-生成的多項式である．

実際，体 k の標数が n と互いに素の場合には，次の様にして $q_2,\ldots,q_{n-1}$ を $s_1,\ldots,s_n$ を用いて表わすことができる：まず，最初に $\mathbf{X}:=(X_1,\ldots,X_n)$，

$$X_1:=x_1-s_1/n,\ X_2:=x_2-s_1/n,\ \ldots,\ X_n:=x_n-s_1/n$$

と置けば，$k(\mathbf{X}):=k(X_1,\ldots,X_{n-1})\subset k(\mathbf{x})$ 及び

$$X_1+X_2+\cdots+X_n=0$$

が得られる．体 $k(\mathbf{x})$ への $\mathfrak{S}_n$-作用は $k(\mathbf{X})$ への線型かつ忠実な作用を引き起こし，また等式 $k(\mathbf{X})^{\mathfrak{S}_n}=k(\mathbf{S}):=k(S_1,S_2,\ldots,S_n)$ を得る．但し，S_i は $X_1,\ldots,X_n$ に関する i 次基本対称式．特に，$S_1=0$ である．多項式 $f_n(\mathbf{S};X)$ と $f_n(\mathbf{s};X)$ は $k(\mathbf{s})$ 上チルンハウス同値となり，$f_n(\mathbf{S};X)$ は体の拡大 $k(\mathbf{X})/k(\mathbf{X})^{\mathfrak{S}_n}$ を生成する．特に，Kemper-Mattig の定理 [KM00] により，$f_n(\mathbf{S};X)$ は $\mathfrak{S}_n$ に対するパラメータ $S_2,\ldots,S_n$ 付きの k-生成的多項式である．そこで

$$q_1:=S_n/S_{n-1},\quad q_i:=S_i/q_1^i,\ (i=2,\ldots,n-1)$$

と定義すれば，$k(\mathbf{S})=k(q_1,\ldots,q_{n-1})$ かつ

$$g_n(q_2,\ldots,q_{n-1};X)=(-1/q_1)^n f_n(\mathbf{S};-q_1X)$$

が得られ，$g_n(q_2,\ldots,q_{n-1};X)$ と $f_n(\mathbf{S};X)$ は $k(\mathbf{S})$ 上チルンハウス同値である．また $\deg(q_1)=1$，$\deg(q_i)=0,(i=2,\ldots,n-1)$ であることから，$g_n(q_2,\ldots,q_{n-1};X)$ は次数 0 の体 $k(\mathbf{X})_0:=k(X_1/X_2,\ldots,X_{n-1}/X_n)\subset k(\mathbf{X})$ を体 $k(\mathbf{X})_0^{\mathfrak{S}_n}=k(q_2,\ldots,q_{n-1})$ 上生成する (cf. [Kem96], [KM00, Theorem7])．

系 3.11.　体 $M=k(q_2,\ldots,q_{n-1},r_2,\ldots,r_{n-1})$ を k 上の $2(n-2)$ 変数有理関数体とする．また $\mathbf{a}=(0,q_2,\ldots,q_{n-1},q_{n-1})\in M^n$，$\mathbf{b}=(0,r_2,\ldots,r_{n-1},r_{n-1})\in M^n$ とする．ある $j,(0\le j\le n-1)$，に対して，$F_j(\mathbf{a},\mathbf{b};X)\in M[X]$ が重根を持たなければ，$F_j(\mathbf{a},\mathbf{b};X)$ は $\mathfrak{S}_n\times\mathfrak{S}_n$ に対する $2(n-2)$ 個のパラメータ $q_2,\ldots,q_{n-1},r_2,\ldots,r_{n-1}$ を持つ k-生成的多項式である．

生成的多項式の部分体問題の解を得るために，各 $g\in G_{\mathbf{s},\mathbf{t}}$ に対してチルンハウス変換の係数体 $M(c_0^g,\ldots,c_{n-1}^g)$ の M 上の次数を考察する．我々の多項式 $F_i(\mathbf{a},\mathbf{b};X)$ の M 上の既約多項式への因数分解の型は，特殊化 $(\mathbf{s},\mathbf{t})\mapsto(\mathbf{a},\mathbf{b})$ による $f_n(\mathbf{a};X)$ と $f_n(\mathbf{b};X)$ のガロア群の退化の様子，及び $f_n(\mathbf{a};X)$ と $f_n(\mathbf{b};X)$ の M 上の根体の共通部分の大きさを，命題 3.2 のようにして，体 $M(c_0^g,\ldots,c_{n-1}^g)$ の M 上の次数を通じて我々に教えてくれる．

命題 3.12.　体 M の標数が 2 でない場合には $\Delta_{\mathbf{a}}/\Delta_{\mathbf{b}} \in M$，標数が 2 の場合には $\beta_{\mathbf{a}} + \beta_{\mathbf{b}} \in M$ とする．このとき多項式 $F_i(\mathbf{a}, \mathbf{b}; X)$ は次数 $n!/2$ の 2 つの因子に M 上で分解する．但し，これら 2 つの多項式は M 上既約であるとは限らない．

証明.　命題 2.7 から従う．　□

系 3.13.　もし $G_{\mathbf{a}}, G_{\mathbf{b}} \subset \mathfrak{A}_n$ であれば，$F_i(\mathbf{a}, \mathbf{b}; X)$ は（M 上既約であるとは限らない）次数 $n!/2$ の 2 つの因子に M 上で分解する．

§4.　3 次多項式の場合

これまでの §2, §3 における一般論を基にして，生成的多項式の部分体問題を 3 次の場合に限定し，より具体的に考察する．多項式

$$f_3(\mathbf{s}; X) := X^3 - s_1X^2 + s_2X - s_3 \in k(\mathbf{s})[X],$$

$$\begin{aligned} s_1 &= x_1 + x_2 + x_3, \\ s_2 &= x_1x_2 + x_1x_3 + x_2x_3, \\ s_3 &= x_1x_2x_3 \end{aligned}$$

を用意し，§3 の様に差積 $\Delta_{\mathbf{s}}$，または $\mathrm{char}\, k = 2$ の場合には Berlekamp の判別式 $\beta_{\mathbf{s}}$ を取る：

$$\begin{aligned} \Delta_{\mathbf{s}} &:= (x_2 - x_1)(x_3 - x_1)(x_3 - x_2), \\ \beta_{\mathbf{s}} &:= \frac{x_1}{x_1 + x_2} + \frac{x_1}{x_1 + x_3} + \frac{x_2}{x_2 + x_3} \\ &= \frac{x_1^2x_2 + x_2^2x_3 + x_1x_3^2 + x_1x_2x_3}{x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1x_2^2 + x_2x_3^2 + x_3x_1^2}. \end{aligned} \tag{11}$$

差積 $\Delta_{\mathbf{s}}$，Berlekamp の判別式 $\beta_{\mathbf{s}}$ はそれぞれ

$$\begin{aligned} \Delta_{\mathbf{s}}^2 &= s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 + 18s_1s_2s_3 - 27s_3^2, \\ \beta_{\mathbf{s}}(\beta_{\mathbf{s}} + 1) &= \frac{s_2^3 + s_1^3s_3 + s_1s_2s_3 + s_3^2}{s_1^2s_2^2 + s_3^2} \end{aligned}$$

を満たし，体 $k(\mathbf{s})(\Delta_{\mathbf{s}})$（$k$ の標数が 2 の場合には $k(\mathbf{s})(\beta_{\mathbf{s}})$）は $k(\mathbf{s})$ の 2 次拡大となる．剰余類 $\overline{g} = \overline{(1, \tau)} \in H\backslash G_{\mathbf{s},\mathbf{t}}$ に対応させて，

$$\begin{pmatrix} u_0^g \\ u_1^g \\ u_2^g \end{pmatrix} := \begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix}^{-1} \begin{pmatrix} y_1^\tau \\ y_2^\tau \\ y_3^\tau \end{pmatrix}$$

と置く．定義から (u_0, u_1, u_2) は次の形のように直接計算できる．

$$
\begin{aligned}
u_0 &= \Delta_{\mathbf{s}}^{-1}\cdot\det\begin{pmatrix} y_1 & x_1 & x_1^2 \\ y_2 & x_2 & x_2^2 \\ y_3 & x_3 & x_3^2 \end{pmatrix} \\
&= \frac{x_2x_3y_1}{(x_2-x_1)(x_3-x_1)} - \frac{x_1x_3y_2}{(x_2-x_1)(x_3-x_2)} + \frac{x_1x_2y_3}{(x_3-x_1)(x_3-x_2)}, \\
u_1 &= \Delta_{\mathbf{s}}^{-1}\cdot\det\begin{pmatrix} 1 & y_1 & x_1^2 \\ 1 & y_2 & x_2^2 \\ 1 & y_3 & x_3^2 \end{pmatrix} \\
&= -\frac{(x_2+x_3)y_1}{(x_2-x_1)(x_3-x_1)} + \frac{(x_1+x_3)y_2}{(x_2-x_1)(x_3-x_2)} - \frac{(x_1+x_2)y_3}{(x_3-x_1)(x_3-x_2)}, \\
u_2 &= \Delta_{\mathbf{s}}^{-1}\cdot\det\begin{pmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{pmatrix} \\
&= \frac{y_1}{(x_2-x_1)(x_3-x_1)} - \frac{y_2}{(x_2-x_1)(x_3-x_2)} + \frac{y_3}{(x_3-x_1)(x_3-x_2)}.
\end{aligned}
$$

多項式 $f_3(\mathbf{s};X)$ のチルンハウス変換の一般形は

$$
\begin{aligned}
&g_3(\mathbf{s},u_0,u_1,u_2;X) \\
&:= \mathrm{Resultant}_Y\big(f_3(\mathbf{s};Y), X-(u_0+u_1Y+u_2Y^2)\big) \\
&= X^3+(-3u_0-s_1u_1-s_1^2u_2+2s_2u_2)X^2+(3u_0^2+2s_1u_0u_1+s_2u_1^2 \\
&\quad +2s_1^2u_0u_2-4s_2u_0u_2+s_1s_2u_1u_2-3s_3u_1u_2+s_2^2u_2^2-2s_1s_3u_2^2)X \\
&\quad -u_0^3-s_1u_0^2u_1-s_2u_0u_1^2-s_3u_1^3-s_1^2u_0^2u_2+2s_2u_0^2u_2-s_1s_2u_0u_1u_2 \\
&\quad +3s_3u_0u_1u_2-s_1s_3u_1^2u_2-s_2^2u_0u_2^2+2s_1s_3u_0u_2^2-s_2s_3u_1u_2^2-s_3^2u_2^3
\end{aligned}
\tag{12}
$$

によって与えられる．また，定義から u_0,u_1,u_2 は

$$
f_3(\mathbf{t};X) = g_3(\mathbf{s},u_0^g,u_1^g,u_2^g;X), \quad (g\in G_{\mathbf{s},\mathbf{t}}) \tag{13}
$$

を満たす．以下において，便宜上，記号

$$
\begin{aligned}
A_{\mathbf{s}} &:= s_1^2-3s_2, \\
B_{\mathbf{s}} &:= 2s_1^3-9s_1s_2+27s_3, \\
C_{\mathbf{s}} &:= s_1^4-4s_1^2s_2+s_2^2+6s_1s_3, \\
D_{\mathbf{s}} &:= \mathrm{Disc}_X f_3(\mathbf{s};X) = s_1^2s_2^2-4s_2^3-4s_1^3s_3+18s_1s_2s_3-27s_3^2 \quad (=\Delta_{\mathbf{s}}^2)
\end{aligned}
\tag{14}
$$

を使う事にする．直接計算から等式

$$4A_{\mathbf{s}}^3 - B_{\mathbf{s}}^2 = 27D_{\mathbf{s}} \tag{15}$$

が成り立つことが確かめられる．計算代数を用いて，6 次多項式

$$F_i(\mathbf{s},\mathbf{t};X) = \prod_{\overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}} (X - u_i^g) \in K[X], \quad (i=1,2)$$

を求めると以下のようになる：

$$\begin{aligned} F_1(\mathbf{s},\mathbf{t};X) := X^6 &- \frac{2A_{\mathbf{t}}C_{\mathbf{s}}}{D_{\mathbf{s}}}X^4 - \frac{(s_1s_2-s_3)B_{\mathbf{t}}}{D_{\mathbf{s}}}X^3 + \frac{A_{\mathbf{t}}^2C_{\mathbf{s}}^2}{D_{\mathbf{s}}^2}X^2 \\ &+ \frac{(s_1s_2-s_3)A_{\mathbf{t}}B_{\mathbf{t}}C_{\mathbf{s}}}{D_{\mathbf{s}}^2}X + \frac{(s_1s_2-s_3)^2A_{\mathbf{t}}^3D_{\mathbf{s}} - C_{\mathbf{s}}^3D_{\mathbf{t}}}{D_{\mathbf{s}}^3}, \end{aligned} \tag{16}$$

$$\begin{aligned} F_2(\mathbf{s},\mathbf{t};X) := X^6 &- \frac{2A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X^4 + \frac{B_{\mathbf{t}}}{D_{\mathbf{s}}}X^3 \\ &+ \frac{A_{\mathbf{s}}^2A_{\mathbf{t}}^2}{D_{\mathbf{s}}^2}X^2 - \frac{A_{\mathbf{s}}A_{\mathbf{t}}B_{\mathbf{t}}}{D_{\mathbf{s}}^2}X + \frac{A_{\mathbf{t}}^3D_{\mathbf{s}} - A_{\mathbf{s}}^3D_{\mathbf{t}}}{D_{\mathbf{s}}^3}; \end{aligned} \tag{17}$$

但し $A_{\mathbf{s}}, B_{\mathbf{s}}, C_{\mathbf{s}}, D_{\mathbf{s}}$ の定義は式 (14) による．多項式 $F_0(\mathbf{s},\mathbf{t};X)$ の表示は，その根 u_0^g が $F_1(\mathbf{s},\mathbf{t};X)$ と $F_2(\mathbf{s},\mathbf{t};X)$ の根から式 (20) と (26) を用いて得られることもあり，複雑なので省略する．多項式 $F_2(\mathbf{s},\mathbf{t};X)$ の X に関する判別式は

$$D_{\mathbf{s},\mathbf{t}} := \frac{B_{\mathbf{s}}^6D_{\mathbf{t}}^3(A_{\mathbf{s}}^3B_{\mathbf{t}}^2 - 27A_{\mathbf{t}}^3D_{\mathbf{s}})^2}{D_{\mathbf{s}}^{15}} \tag{18}$$

で与えられる．また，char $k \neq 2$ の場合には，式 (15) から次のようにも表示できる：

$$A_{\mathbf{s}}^3B_{\mathbf{t}}^2 - 27A_{\mathbf{t}}^3D_{\mathbf{s}} = 4A_{\mathbf{s}}^3A_{\mathbf{t}}^3 - 27(A_{\mathbf{t}}^3D_{\mathbf{s}} + A_{\mathbf{s}}^3D_{\mathbf{t}}) = \frac{B_{\mathbf{s}}^2B_{\mathbf{t}}^2 - 3^6D_{\mathbf{s}}D_{\mathbf{t}}}{4}. \tag{19}$$

命題 2.7 より $F_2(\mathbf{s},\mathbf{t};X)$ の分解

$$F_2(\mathbf{s},\mathbf{t};X) = F_2^+(X)F_2^-(X)$$

が得られる．但し $F_2^+(X)$, $F_2^-(X)$ は $K(\Delta_{\mathbf{s}}/\Delta_{\mathbf{t}})$ 上 (char $k=2$ のときは $K(\beta_{\mathbf{s}}+\beta_{\mathbf{t}})$ 上) 定義された多項式である．

まず char $k \neq 2$ なる場合には，定義 (4) より

$$F_2^+(X) = \prod_{\substack{\overline{(1,\tau)}\in H\backslash G_{\mathbf{s},\mathbf{t}} \\ \psi(\tau)\in\mathfrak{A}_3}} (X - u_2^{(1,\tau)}) = X^3 - \frac{A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X + \frac{B_{\mathbf{t}} - B_{\mathbf{s}}(\Delta_{\mathbf{t}}/\Delta_{\mathbf{s}})}{2D_{\mathbf{s}}},$$

$$F_2^-(X) = \prod_{\substack{\overline{(1,\tau)}\in H\backslash G_{\mathbf{s},\mathbf{t}} \\ \psi(\tau)\notin\mathfrak{A}_3}} (X - u_2^{(1,\tau)}) = X^3 - \frac{A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X + \frac{B_{\mathbf{t}} + B_{\mathbf{s}}(\Delta_{\mathbf{t}}/\Delta_{\mathbf{s}})}{2D_{\mathbf{s}}}$$

である．

また char $k=2$ の場合には，

$$F_2^+(X) = X^3 + \frac{A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X + \frac{s_1A_{\mathbf{s}}B_{\mathbf{t}} + t_1A_{\mathbf{t}}B_{\mathbf{s}} + B_{\mathbf{s}}B_{\mathbf{t}}(\beta_{\mathbf{s}}+\beta_{\mathbf{t}})}{B_{\mathbf{s}}D_{\mathbf{s}}},$$
$$F_2^-(X) = X^3 + \frac{A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X + \frac{s_1A_{\mathbf{s}}B_{\mathbf{t}} + t_1A_{\mathbf{t}}B_{\mathbf{s}} + B_{\mathbf{s}}B_{\mathbf{t}}(\beta_{\mathbf{s}}+\beta_{\mathbf{t}}+1)}{B_{\mathbf{s}}D_{\mathbf{s}}}$$

が得られる．

無限体 M に対して，特殊化 $(\mathbf{s},\mathbf{t}) \mapsto (\mathbf{a},\mathbf{b}) \in M^3 \times M^3$ は，常に $f_3(\mathbf{a};X)$, $f_3(\mathbf{b};X)$ が M 上分離的になるように選ばれるものと前提する．すなわち，以下 $D_{\mathbf{a}} \cdot D_{\mathbf{b}} \neq 0$ を仮定する．また

$$L_{\mathbf{a}} := \mathrm{Spl}_M f_3(\mathbf{a};X), \qquad L_{\mathbf{b}} := \mathrm{Spl}_M f_3(\mathbf{b};X),$$
$$G_{\mathbf{a}} := \mathrm{Gal}(L_{\mathbf{a}}/M), \qquad G_{\mathbf{b}} := \mathrm{Gal}(L_{\mathbf{b}}/M)$$

と置き，$\#G_{\mathbf{a}} \geq \#G_{\mathbf{b}}$ であるとする．さらに，$f_3(\mathbf{a};X)$ は M 上既約であると仮定する．群 $G_{\mathbf{a}}$ は $\mathfrak{S}_3$ または $\mathfrak{A}_3 = C_3$ と同型であり，群 $G_{\mathbf{b}}$ は $\mathfrak{S}_3, C_3, C_2$ または $\{1\}$ と同型となる．我々は $F_j(\mathbf{s},\mathbf{t};X)$ を通して $f_3(\mathbf{s};X)$ に対する部分体問題の解を与える．すなわち $\mathbf{a},\mathbf{b} \in M^3$ に対し，$L_{\mathbf{a}} \supseteq L_{\mathbf{b}}$ となる必要十分条件を与える．

4.1　char $k \neq 3$ の場合．

最初に，体 k の標数が 3 ではない場合を取り扱い，char $k = 3$ の場合は小節 4.4 で論じる．

式 (13) の多項式を X について展開し，各項を比較することで

$$u_0 = \frac{t_1 - s_1u_1 - s_1^2u_2 + 2s_2u_2}{3}, \quad u_1 = \frac{Q_{1,2}(\mathbf{s},\mathbf{t};u_2)}{D_{1,2}(\mathbf{s},\mathbf{t};u_2)} \tag{20}$$

但し，

$$Q_{1,2}(\mathbf{s},\mathbf{t};u_2) := 3A_{\mathbf{s}}^2B_{\mathbf{t}} - A_{\mathbf{t}}(6A_{\mathbf{s}}^3 - B_{\mathbf{s}}^2 + 2A_{\mathbf{s}}B_{\mathbf{s}}s_1)u_2 + 6D_{\mathbf{s}}(A_{\mathbf{s}}^2 + B_{\mathbf{s}}s_1)u_2^3,$$
$$D_{1,2}(\mathbf{s},\mathbf{t};u_2) := 3B_{\mathbf{s}}(A_{\mathbf{s}}A_{\mathbf{t}} - 3D_{\mathbf{s}}u_2^2)$$

が得られる．また，u_1 を消去することによって

$$u_0 = \frac{(t_1 - s_1^2u_2 + 2s_2u_2)D_{1,2}(\mathbf{s},\mathbf{t};u_2) - s_1Q_{1,2}(\mathbf{s},\mathbf{t};u_2)}{3D_{1,2}(\mathbf{s},\mathbf{t};u_2)} \tag{21}$$

が得られる．

式 (20) と (21) から，命題 2.2 のようにして，任意の $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$K(u_0^g, u_1^g, u_2^g) = K(u_2^g)$, $K = k(\mathbf{s},\mathbf{t})$ であることが直接確認できる．さらには，式 (10) を満たす $D_{0,2}^0(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ と $D_{1,2}^0(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ が次のように得られる：まず，

$$\frac{1}{D_{1,2}(\mathbf{s},\mathbf{t};u_2)} = \frac{1}{3B_{\mathbf{s}}(A_{\mathbf{s}}A_{\mathbf{t}} - 3D_{\mathbf{s}}u_2^2)} = \frac{1}{D_{1,2}^0(\mathbf{s},\mathbf{t})}\sum_{i=0}^{5} h_i(\mathbf{s},\mathbf{t})u_2^i$$

となる $D_{1,2}^0(\mathbf{s},\mathbf{t})$, $h_i(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ を取る．実際，計算代数を用いて

$$D^0_{1,2}(\mathbf{s},\mathbf{t}) := 3B_\mathbf{s}(A^3_\mathbf{s}B^2_\mathbf{t} - 27A^3_\mathbf{t}D_\mathbf{s})^2$$

かつ

$$\begin{aligned}
&\{h_0(\mathbf{s},\mathbf{t}),\dots,h_5(\mathbf{s},\mathbf{t})\}\\
&\quad=\Big\{4A^2_\mathbf{s}A^2_\mathbf{t}(A^3_\mathbf{s}B^2_\mathbf{t}+27A^3_\mathbf{t}D_\mathbf{s}-27B^2_\mathbf{t}D_\mathbf{s}),\\
&\qquad 27B_\mathbf{t}D_\mathbf{s}(4A^3_\mathbf{s}A^3_\mathbf{t}+9A^3_\mathbf{t}D_\mathbf{s}-9A^3_\mathbf{s}D_\mathbf{t}),\\
&\qquad -3A_\mathbf{s}A_\mathbf{t}D_\mathbf{s}(5A^3_\mathbf{s}B^2_\mathbf{t}+135A^3_\mathbf{t}D_\mathbf{s}-54B^2_\mathbf{t}D_\mathbf{s}),\\
&\qquad -270A^2_\mathbf{s}A^2_\mathbf{t}B_\mathbf{t}D^2_\mathbf{s},\ 9D^2_\mathbf{s}(A^3_\mathbf{s}B^2_\mathbf{t}+27A^3_\mathbf{t}D_\mathbf{s}),\ 162A_\mathbf{s}A_\mathbf{t}B_\mathbf{t}D^3_\mathbf{s}\Big\}
\end{aligned}$$

を得ることができる．ここで，式 (21) から，$D^0_{0,2}(\mathbf{s},\mathbf{t}) := 3\cdot D^0_{1,2}(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ と定義する．以上によって，

$$u_i = \frac{1}{D^0_{i,2}(\mathbf{s},\mathbf{t})}\,P^0_{i,2}(\mathbf{s},\mathbf{t};u_2),\quad \text{かつ}\quad \deg_X(P^0_{i,2}(\mathbf{s},\mathbf{t};X)) = 5$$

を満たす $P^0_{i,2}(\mathbf{s},\mathbf{t};X) \in k[\mathbf{s},\mathbf{t}][X], (i=0,1)$, が具体的に得られる．

変数の特殊化 $(\mathbf{s},\mathbf{t}) \mapsto (\mathbf{a},\mathbf{b}) \in M^3\times M^3$ においては，次の補題が成り立つ．

補題 4.1. (1) もし $f_3(\mathbf{a};X)$ が M 上既約ならば，$B_\mathbf{a}\neq 0$.
(2) もし $A_\mathbf{a}=0$ ならば，$f_3(\mathbf{a};X)$ と $X^3-B_\mathbf{a}$ は M 上チルンハウス同値である．よって，$f_3(\mathbf{a};X)$ の $M(\sqrt{-3})$ 上のガロア群は位数 3 の巡回群となる．
(3) もし $A_\mathbf{a}=0$ ならば，$f_3(\mathbf{a};X)$ と $Y^3-3Y-(B_\mathbf{a}+1/B_\mathbf{a})$ は M 上チルンハウス同値である．

証明. (1) および (2) は等式

$$3^3\cdot f_3(\mathbf{s};X) = (3X-s_1)^3 - 3A_\mathbf{s}(3X-s_1) - B_\mathbf{s}$$

から従う．$X^3-B_\mathbf{a}=0$ である場合には，$Y = X+1/X = X(1+X/B_\mathbf{a})$ と置くことによって $Y^3-3Y-(B_\mathbf{a}+1/B_\mathbf{a})=0$ を得る． □

補題 4.1 (1) によって，$f_3(\mathbf{a};X)$ が M 上既約という仮定から $B_\mathbf{a}\neq 0$ が従う．また，補題 4.1 (3) により，一般性を失うことなく，$A_\mathbf{a}\neq 0$ かつ $A_\mathbf{b}\neq 0$ と仮定してよい．

式 (18) と $B_\mathbf{a}\neq 0$ かつ $D_\mathbf{b}\neq 0$ という仮定の下では，多項式 $F_2(\mathbf{a},\mathbf{b};X)$ が重根をもつためには，$A^3_\mathbf{a}B^2_\mathbf{b}-27A^3_\mathbf{b}D_\mathbf{a}=0$ が必要十分であることが分かる．

補題 4.2. (1) もし $A^3_\mathbf{a}B^2_\mathbf{b}-27A^3_\mathbf{b}D_\mathbf{a}=0$ ならば，$F_2(\mathbf{a},\mathbf{b};X)$ は M 上次のように因数分解する：

$$F_2(\mathbf{a},\mathbf{b};X) = \Big(X-\frac{3A^2_\mathbf{b}}{A_\mathbf{a}B_\mathbf{b}}\Big)^2\Big(X+\frac{6A^2_\mathbf{b}}{A_\mathbf{a}B_\mathbf{b}}\Big)\Big(X^3-\frac{27A^4_\mathbf{b}X}{A^2_\mathbf{a}B^2_\mathbf{b}}-\frac{27A^3_\mathbf{b}(2A^3_\mathbf{b}-B^2_\mathbf{b})}{A^3_\mathbf{a}B^3_\mathbf{b}}\Big);$$

但し，最後の項は M 上既約である．

(2) もし $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=0$ ならば，$F_2(\mathbf{a},\mathbf{b};X)$ の重根 $c=3A_{\mathbf{b}}^2/(A_{\mathbf{a}}B_{\mathbf{b}})$ は $A_{\mathbf{a}}A_{\mathbf{b}}-3D_{\mathbf{a}}c^2=0$ を満たす．逆に，$F_2(\mathbf{a},\mathbf{b};X)$ の根 c が $A_{\mathbf{a}}A_{\mathbf{b}}-3D_{\mathbf{a}}c^2=0$ を満たすならば，$A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=0$ が成り立つ．

証明. [HM] 参照. □

前節 § 3 における，定理 3.8 および系 3.9 の特別な場合として，k-生成的多項式 $f_3(\mathbf{s};X)$ の同型問題への解が次のようにして得られる．

定理 4.3. (1) もし $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=0$ ならば，$\mathrm{Spl}_M f_3(\mathbf{a};X)=\mathrm{Spl}_M f_3(\mathbf{b};X)$.

(2) もし $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}\neq 0$ ならば，次の 2 つの条件は同値である：

(i) $\mathrm{Spl}_M f_3(\mathbf{a};X)=\mathrm{Spl}_M f_3(\mathbf{b};X)$;

(ii) 6 次多項式 $F_2(\mathbf{a},\mathbf{b};X)$ は M 内に根を持つ．

証明. (1) $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=0$ である場合は，補題 4.2 から，ある $g\in G_{\mathbf{s},\mathbf{t}}$ に対して $c_2^g=-(6A_{\mathbf{b}}^2)/(A_{\mathbf{a}}B_{\mathbf{b}})\in M$ となる．このとき，$D_{1,2}(\mathbf{a},\mathbf{b};c_2^g)=3B_{\mathbf{a}}(A_{\mathbf{a}}A_{\mathbf{b}}-3D_{\mathbf{a}}(c_2^g)^2)=-9B_{\mathbf{a}}A_{\mathbf{a}}A_{\mathbf{b}}\neq 0$ が成り立つ．よって，式 (20) および式 (21) より $M(c_0^g,c_1^g,c_2^g)=M(c_2^g)=M$ が得られる．

(2) もし $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}\neq 0$ ならば，$D_{0,2}^0(\mathbf{a},\mathbf{b})\cdot D_{1,2}^0(\mathbf{a},\mathbf{b})\neq 0$ が従う．よってこの主張は定理 3.8 (または系 3.9) から従う． □

例 4.4. ここで，等式 $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=0$ が満たされる場合の例を 2 つ挙げておく．

(1) $M=\mathbb{Q}$ として，$\mathbf{a}=(0,3,-2)$, $\mathbf{b}=(3,-3,3)\in M$ をとる．このとき，

$$f_3(\mathbf{a};X)=X^3+3X+2,\quad f_3(\mathbf{b};X)=X^3-3X^2-3X-3$$

および $(A_{\mathbf{a}},B_{\mathbf{a}},C_{\mathbf{a}},D_{\mathbf{a}})=(-9,-54,9,-216)$, $(A_{\mathbf{b}},B_{\mathbf{b}},D_{\mathbf{b}})=(18,216,-864)$ が得られる．多項式 $f_3(\mathbf{a};X)$ と $f_3(\mathbf{b};X)$ は共に $\mathbb{Q}$ 上既約であり，しかも $D_{\mathbf{a}}=-2^3\cdot 3^3$ と $D_{\mathbf{b}}=-2^5\cdot 3^3$ は $M=\mathbb{Q}$ の中で平方数ではないので，$f_3(\mathbf{a};X)$ と $f_3(\mathbf{b};X)$ の $\mathbb{Q}$ 上のガロア群は共に 3 次対称群 $\mathfrak{S}_3$ と同型である．また $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=0$ であることも直接計算によって確かめられる．補題 4.2 (1) より

$$F_2(\mathbf{a},\mathbf{b};X)=\Big(X+\frac{1}{2}\Big)^2\Big(X-1\Big)\Big(X^3-\frac{3X}{4}-\frac{3}{4}\Big)$$

が得られる．よって $c_2^g=1$ を採ると，式 (20), (21) から $(c_0^g,c_1^g,c_2^g)=(3,-1,1)$ が分かる．これにより $\mathbb{Q}[X]/(f_3(\mathbf{a};X))\cong_{\mathbb{Q}}\mathbb{Q}[X]/(f_3(\mathbf{b};X))$．さらに，$f_3(\mathbf{a};X)$ から $f_3(\mathbf{b};X)$ への $\mathbb{Q}$ 上のチルンハウス変換は具体的に

$$f_3(\mathbf{b};Y)=\mathrm{Resultant}_X(f_3(\mathbf{a};X),Y-(3-X+X^2))$$

として与えられる．また

$$F_1(\mathbf{a},\mathbf{b};X) = \Big(X^2 - X + \frac{7}{4}\Big)\Big(X+1\Big)\Big(X^3 + \frac{3X}{4} + \frac{1}{4}\Big),$$
$$F_0(\mathbf{a},\mathbf{b};X) = X^2(X-3)(X^3 - 3X^2 - 4)$$

も得られる．

(2) $M = \mathbb{Q}$ として，$\mathbf{a} = (-3,-4,-1)$, $\mathbf{b} = (-1,-2,1) \in M$ をとる．このとき，

$$f_3(\mathbf{a};X) = X^3 + 3X^2 - 4X + 1, \quad f_3(\mathbf{b};X) = X^3 + X^2 - 2X - 1$$

であり，$(A_\mathbf{a}, B_\mathbf{a}, C_\mathbf{a}, D_\mathbf{a}) = (21,-189,259,49)$, $(A_\mathbf{b}, B_\mathbf{b}, D_\mathbf{b}) = (7,7,49)$ である．また $f_3(\mathbf{a};X)$ と $f_3(\mathbf{b};X)$ は共に $\mathbb{Q}$ 上既約であり，$D_\mathbf{a} = D_\mathbf{b} = 7^2$ であることから，$f_3(\mathbf{a};X)$ と $f_3(\mathbf{b};X)$ の $\mathbb{Q}$ 上のガロア群は共に 3 次巡回群 C_3 と同型になる．さらに $A_\mathbf{a}^3 B_\mathbf{b}^2 - 27A_\mathbf{b}^3 D_\mathbf{a} = 0$ であり，補題 4.2 (1) から

$$F_2(\mathbf{a},\mathbf{b};X) = \Big(X-1\Big)^2\Big(X+2\Big)\Big(X^3 - 3X - \frac{13}{7}\Big)$$

が得られる．よって $c_2^g = -2$ を取れば，式 (20) と (21) から $(c_0^g, c_1^g, c_2^g) = (4,-7,-2)$ が直接計算できる．これより $\mathbb{Q}[X]/(f_3(\mathbf{a};X)) \cong_\mathbb{Q} \mathbb{Q}[X]/(f_3(\mathbf{b};X))$．また $f_3(\mathbf{a};X)$ から $f_3(\mathbf{b};X)$ への $\mathbb{Q}$ 上の具体的なチルンハウス変換は

$$f_3(\mathbf{b};Y) = \mathrm{Resultant}_X(f_3(\mathbf{a};X), Y - (4 - 7X - 2X^2))$$

によって与えられる．さらに

$$F_1(\mathbf{a},\mathbf{b};X) = \Big(X-3\Big)\Big(X-4\Big)\Big(X+7\Big)\Big(X^3 - 37X - \frac{601}{7}\Big),$$
$$F_0(\mathbf{a},\mathbf{b};X) = \Big(X+3\Big)\Big(X+2\Big)\Big(X-4\Big)\Big(X^3 + X^2 - 14X + \frac{71}{7}\Big)$$

も得られる．これから，$f_3(\mathbf{a};X)$ から $f_3(\mathbf{b};X)$ への $\mathbb{Q}$ 上定義された，3 つのチルンハウス変換のうち，残り 2 つは

$$f_3(\mathbf{b};Y) = \mathrm{Resultant}_X(f_3(\mathbf{a};X), Y - (-3 + 3X + X^2)),$$
$$f_3(\mathbf{b};Y) = \mathrm{Resultant}_X(f_3(\mathbf{a};X), Y - (-2 + 4X + X^2))$$

によって具体的に与えられることが分かる．

我々の目標である，k-生成的多項式 $f_3(\mathbf{s};X)$ の部分体問題の解は，次のようにして与えられる．

定理 4.5. 条件 $A_\mathbf{a}^3 B_\mathbf{b}^2 - 27A_\mathbf{b}^3 D_\mathbf{a} \neq 0$ を満たす $\mathbf{a},\mathbf{b} \in M^3$ に対して，$F_2(\mathbf{a},\mathbf{b};X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型により，生成的多項式 $f_3(\mathbf{s};X)$ の部分体問題の解は表 1 のように与えられる．また，各既約因子 $h_\mu(X)$ の根体 M_μ は $\mathrm{Spl}_{M_\mu} f_3(\mathbf{a},X) = \mathrm{Spl}_{M_\mu} f_3(\mathbf{b},X)$ を満たす．

表 1

$G_{\mathbf{a}}$	$G_{\mathbf{b}}$		$(d_\mu), d_\mu = \deg(h_\mu(X))$
$\mathfrak{S}_3$	$\mathfrak{S}_3$	$L_{\mathbf{a}} \neq L_{\mathbf{b}}, L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	(6)
		$L_{\mathbf{a}} \neq L_{\mathbf{b}}, [L_{\mathbf{a}} \cap L_{\mathbf{b}} : K] = 2$	(3)(3)
		$L_{\mathbf{a}} = L_{\mathbf{b}}$	(1)(2)(3)
	C_3	$L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	(6)
	C_2	$L_{\mathbf{a}} \not\supset L_{\mathbf{b}}$	(6)
		$L_{\mathbf{a}} \supset L_{\mathbf{b}}$	(3)(3)
	$\{1\}$	$L_{\mathbf{a}} \supset L_{\mathbf{b}}$	(6)
C_3	C_3	$L_{\mathbf{a}} \neq L_{\mathbf{b}}$	(3)(3)
		$L_{\mathbf{a}} = L_{\mathbf{b}}$	(1)(1)(1)(3)
	C_2	$L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	(6)
	$\{1\}$	$L_{\mathbf{a}} \supset L_{\mathbf{b}}$	(3)(3)

証明. 命題 3.2 と仮定 $A_{\mathbf{a}}^3 B_{\mathbf{b}}^2 - 27 A_{\mathbf{b}}^3 D_{\mathbf{a}} \neq 0$ から，

$$L_{\mathbf{a}} L_{\mathbf{b}} = L_{\mathbf{a}}\, M(c_2^g) = L_{\mathbf{b}}\, M(c_2^g) \quad \text{for} \quad g \in G_{\mathbf{s},\mathbf{t}} \tag{22}$$

が得られる．よって 2 つの多項式 $f_3(\mathbf{a}; X)$ と $f_3(\mathbf{b}; X)$ は $F_2(\mathbf{a}, \mathbf{b}; X)$ の各既約因子 $h_\mu(X)$ の根体上でチルンハウス同値となる．

(i) $G_{\mathbf{a}} \cong \mathfrak{S}_3$ の場合.

(i-1) もし $L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$ ならば，式 (22) より $[M(c_2^g) : M] = 6$ が従う．よって $F_2(\mathbf{a}, \mathbf{b}; X)$ は M 上既約である．

(i-2) もし $[L_{\mathbf{a}} \cap L_{\mathbf{b}} : M] = 2$ ならば，命題 3.12 より $F_2(\mathbf{a}, \mathbf{b}; X)$ は M 上で 2 つの 3 次因子 $F_2(X)^+$, $F_2(X)^-$ の積に分解する．このとき，式 (22) から $[M(c_2^g) : M] \geq 3$ でなくてはならず，各 3 次因子は既約である．

(i-3) もし $G_{\mathbf{b}} \cong \mathfrak{S}_3$ かつ $L_{\mathbf{a}} = L_{\mathbf{b}}$ ならば，$F_2(\mathbf{a}, \mathbf{b}; X)$ は M 上で 2 つの 3 次因子 $F_2(X)^+$, $F_2(X)^-$ の積に分解する．また，定理 4.3 から，少なくともどちらか 1 つは 1 次因子を持たなくてはならない．よって，命題 3.7 (ii) より，$F_2(\mathbf{a}, \mathbf{b}; X)$ の分解の型は (1)(2)(3) となる．

(ii) $G_{\mathbf{a}} \cong C_3$ の場合.

(ii-1) もし $G_{\mathbf{b}} \cong C_3$ かつ $L_{\mathbf{a}} \neq L_{\mathbf{b}}$ ならば，命題 3.12 から，$F_2(\mathbf{a}, \mathbf{b}; X)$ は M 上で 2 つの 3 次因子 $F_2(X)^+$, $F_2(X)^-$ の積に分解する．このとき，式 (22) から $[M(c_2^g) : M] \geq 3$ でなくてはならず，各 3 次因子は既約となる．

(ii-2) もし $G_{\mathbf{b}} \cong C_3$ かつ $L_{\mathbf{a}} = L_{\mathbf{b}}$ ならば，$F_2(\mathbf{a}, \mathbf{b}; X)$ は M 上で 2 つの 3 次因子 $F_2(X)^+$, $F_2(X)^-$ の積に分解する．また，定理 4.3 から，少なくともどちらか 1 つは 1 次因子を持たなくてはならない．

よって，命題 3.7 (ii) より，$F_2(\mathbf{a},\mathbf{b};X)$ の分解の型は (1)(1)(1)(3) となる．

(ii-3) もし $G_{\mathbf{b}} \cong C_2$ ならば，式 (22) から $[M(c_2^g) : M] = 6$ が従う．よって $F_2(\mathbf{a},\mathbf{b};X)$ は M 上既約である．

(ii-4) もし $G_{\mathbf{b}} \cong \{1\}$ ならば，命題 3.12 から $F_2(\mathbf{a},\mathbf{b};X)$ は M 上で 2 つの 3 次因子 $F_2(X)^+$, $F_2(X)^-$ の積に分解する．このとき，$[M(c_2^g) : M] = 3$ より，各 3 次因子は既約となる．　□

4.2　特別な場合 1 : $X^3 + S_2X - S_3$.

この小節でも char $k \neq 3$ とし，$f_3(0,S_2,S_3;X) = X^3 + S_2X - S_3$ の形で与えらた $\mathfrak{S}_3$ に対する k-生成的多項式を取り扱う．まず $\mathbf{X} := (X_1,X_2,X_3)$,

$$X_1 := x_1 - s_1/3,\ X_2 := x_2 - s_1/3,\ X_3 := x_3 - s_1/3$$

とする．このとき，$k(\mathbf{X}) := k(X_1,X_2,X_3) \subset k(x_1,x_2,x_3)$ かつ $X_1+X_2+X_3 = 0$ である．対称群 $\mathfrak{S}_3$ の $k(x_1,x_2,x_3)$ への作用は，体 $k(\mathbf{X})$ への線型かつ忠実な作用を引き起こす．さらに $\mathbf{S} = (S_1,S_2,S_3)$, S_i は X_1,X_2,X_3 に関する i-次基本対称式，とすると，$k(\mathbf{X})^{\mathfrak{S}_3} = k(\mathbf{S})$ を得る．また S_1,S_2,S_3 に対して，

$$S_1 = 0,\ S_2 = -\frac{A_{\mathbf{s}}}{3} = \frac{-(s_1^2-3s_2)}{3},\ S_3 = \frac{B_{\mathbf{s}}}{27} = \frac{2s_1^3 - 9s_1s_2 + 27s_3}{27}$$

が成り立つ．多項式 $f_3(0,S_2,S_3;X)$ と $f_3(\mathbf{s};X)$ は $k(\mathbf{s})$ 上でチルンハウス同値である．さらに，$f_3(\mathbf{S};X)$ は体の拡大 $k(\mathbf{X})/k(\mathbf{X})^{\mathfrak{S}_3}$ を生成する．変数の特殊化 $\mathbf{s} \mapsto \mathbf{a} = (a_1,a_2,a_3) \in M^3$ については，多項式 $f_3(\mathbf{a};X) = X^3 - a_1X^2 + a_2X - a_3$ と $f_3(0,A_2,A_3;X) = X^3 + A_2X - A_3$ は M 上チルンハウス同値となる．但し $A_2 := -A_{\mathbf{a}}/3$, $A_3 := B_{\mathbf{a}}/27$ である．また $\mathbf{T} := (0,T_2,T_3)$ と置けば，

$$D_{\mathbf{S}} = \mathrm{Disc}_X f_3(0,S_2,S_3;X) = -4S_2^3 - 27S_3^2,$$
$$A_{\mathbf{S}}^3B_{\mathbf{T}}^2 - 27A_{\mathbf{T}}^3D_{\mathbf{S}} = -729(4S_2^3T_2^3 + 27S_3^2T_2^3 + 27S_2^3T_3^2)$$

が得られる．さらに

$$F_0(\mathbf{S},\mathbf{T};X) = X^6 - \frac{8S_2^3T_2}{D_{\mathbf{S}}}X^4 + \frac{8S_2^3T_3}{D_{\mathbf{S}}}X^3 + \frac{16S_2^6T_2^2}{D_{\mathbf{S}}^2}X^2 - \frac{32S_2^6T_2T_3}{D_{\mathbf{S}}^2}X + \frac{64S_2^6(S_3^2T_2^3 - S_2^3T_3^2)}{D_{\mathbf{S}}^3}, \tag{23}$$

$$F_1(\mathbf{S},\mathbf{T};X) = X^6 + \frac{6S_2^2T_2}{D_{\mathbf{S}}}X^4 + \frac{27S_3T_3}{D_{\mathbf{S}}}X^3 + \frac{9S_2^4T_2^2}{D_{\mathbf{S}}^2}X^2 + \frac{81S_2^2S_3T_2T_3}{D_{\mathbf{S}}^2}X + \frac{4S_2^6T_2^3 + 108S_2^3S_3^2T_2^3 + 729S_3^4T_2^3 + 27S_2^6T_3^2}{D_{\mathbf{S}}^3}, \tag{24}$$

$$F_2(\mathbf{S},\mathbf{T};X) = X^6 - \frac{18S_2T_2}{D_{\mathbf{S}}}X^4 + \frac{27T_3}{D_{\mathbf{S}}}X^3 + \frac{81S_2^2T_2^2}{D_{\mathbf{S}}^2}X^2 - \frac{243S_2T_2T_3}{D_{\mathbf{S}}^2}X + \frac{729(S_3^2T_2^3 - S_2^3T_3^2)}{D_{\mathbf{S}}^3} \tag{25}$$

であることが分かる．ここで $F_2^0(S_2,S_3,T_2,T_3;X) := F_2(\mathbf{S},\mathbf{T};X)$ と置けば，次が成り立つ．

定理 4.6.　もし $(A_2,A_3),(B_2,B_3) \in M^2$ に対して $4A_2^3B_2^3+27A_3^2B_2^3+27A_2^3B_3^2 \neq 0$ であるならば，$F_2^0(A_2,A_3,B_2,B_3;X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型によって，生成的多項式 $X^3+S_2X-S_3$ の部分体問題の解は定理 4.5 の表 1 のように与えられる．

4.3　特別な場合 2 : X^3+sX+s.

この小節でも char $k \neq 3$ とする．また，前小節のように $A_2 := -A_{\mathbf{a}}/3, A_3 := B_{\mathbf{a}}/27$ と置く．このとき，$A_{\mathbf{a}} \neq 0$ かつ $B_{\mathbf{a}} \neq 0$ であるような $\mathbf{a}=(a_1,a_2,a_3) \in M^3$ に対して，多項式 $f_3(\mathbf{a};X)$ と $f_3(0,a,-a;X)=X^3+aX+a$ は M 上チルンハウス同値である; 但し

$$a := \frac{A_2^3}{A_3^2} = -\frac{27A_{\mathbf{a}}^3}{B_{\mathbf{a}}^2} = -\frac{27(a_1^2-3a_2)^3}{(2a_1^3-9a_1a_2+27a_3)^2}.$$

これは，次の等式から直接従う：

$$X^3+A_2X-A_3 = -\frac{A_3^3}{A_2^3}\Big(\Big(-\frac{A_2X}{A_3}\Big)^3+a\Big(-\frac{A_2X}{A_3}\Big)+a\Big).$$

注意 4.7.　上記のチルンハウス同値及び前小節のチルンハウス同値は，根のアフィン変換のみによって与えられていることに注意しておく．すなわち，根の 1 次式による変換である．

さて $\mathbf{a}=(0,a,-a) \in M^3$, $\mathbf{b}=(0,b,-b) \in M^3$ とすると，

$$D_{\mathbf{a}} = \mathrm{Disc}_X f_3(0,a,-a;X) = -a^2(4a+27),$$
$$A_{\mathbf{a}}^3B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3D_{\mathbf{a}} = -729a^2b^2(4ab+27a+27b)$$

を得る．

定理 4.5 より，$D_{\mathbf{a}} \cdot D_{\mathbf{b}} \neq 0$ であるような $a,b \in M$ に対し，もし $4ab+27a+27b=0$ ならば，X^3+aX+a と X^3+bX+b は M 上チルンハウス同値である．よって

$$X^3+aX+a \quad と \quad X^3-\frac{27a}{4a+27}X-\frac{27a}{4a+27}$$

は M 上で同じ最小分解体を持つ．

例 4.8.　上の場合，$M=\mathbb{Q}$ とすれば，以下が得られる：

$$\mathrm{Spl}_M(X^3-189X-189) = \mathrm{Spl}_M(X^3-7X-7),$$
$$\mathrm{Spl}_M(X^3-27X-27) = \mathrm{Spl}_M(X^3-9X-9),$$
$$\mathrm{Spl}_M(X^3-6X-6) = \mathrm{Spl}_M(X^3+54X+54).$$

また，

$$F_0(0,s,-s,0,t,-t;X) = X^6 - \frac{8s^3t}{D_s}X^4 - \frac{8s^3t}{D_s}X^3 + \frac{16s^6t^2}{D_s^2}X^2 + \frac{32s^6t^2}{D_s^2}X - \frac{64s^8t^2(s-t)}{D_s^3},$$

$$F_1(0,s,-s,0,t,-t;X) = X^6 + \frac{6s^2t}{D_s}X^4 + \frac{27st}{D_s}X^3 + \frac{9s^4t^2}{D_s^2}X^2 + \frac{81s^3t^2}{D_s^2}X + \frac{s^4t^2(27s^2+729t+108st+4s^2t)}{D_s^3},$$

$$F_2(0,s,-s,0,t,-t;X) = X^6 - \frac{18st}{D_s}X^4 - \frac{27t}{D_s}X^3 + \frac{81s^2t^2}{D_s^2}X^2 + \frac{243st^2}{D_s^2}X - \frac{729s^2t^2(s-t)}{D_s^3}$$

が得られる．但し $D_s = -s^2(4s+27)$ である．ここで $G_2(s,t;X) := F_2(0,s,-s,0,t,-t;X)$ と置けば，次の定理が成り立つ．

定理 4.9. もし $D_a \cdot D_b \neq 0$ であるような $a,b \in M$ に対して $4ab+27a+27b \neq 0$ であれば，$G_2(a,b;X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型によって，生成的多項式 X^3+sX+s の部分体問題の解は定理 4.5 の表 1 のように与えられる．

論文 [HM07] において，我々は char $k \neq 3$ という仮定の下で生成的多項式 X^3+sX+s の同型問題の解を与えた．ここでは，論文 [HM07] の結果を，少し変形させた形で与える ([HM07] の Theorem 1, Theorem 7 を参照)．まず，$G_2(a,b;X)$ が 0 を根に持つ，すなわち $G_2(a,b;0)=0$ ならば，$ab(a-b)=0$ となることに注意する．以下，$a \neq b$ を仮定する．剰余類 $\bar{g} \in H\backslash G_{s,t}$ に対して，$c_2^g \neq 0$ であることから，$u := 3c_1/c_2$ が定義され，$(c_0,c_1) = (2ac_2/3, uc_2/3)$ かつ

$$c_2 = \frac{3(u^2+9u-3a)}{u^3-2au^2-9au-2a^2-27a}$$

が成り立つ．さらに，$a(4a+27) \neq 0$ の仮定の下で，$u^3-2au^2-9au-2a^2-27a \neq 0$ であることが分かる．これより $M(c_0,c_1,c_2) = M(u)$ である．また，直接計算から $(a-b)\cdot\prod_{g\in H\backslash G_{s,t}}(X-u^g) =: H(a,b;X)$ とするとき，

$$H(a,b;X) = a(X^2+9X-3a)^3 - b(X^3-2aX^2-9aX-2a^2-27a)^2$$

が得られる．また $\mathrm{Disc}_X H(a,b;X) = a^{10}b^4(a-b)(4a+27)^{15}(4b+27)^3$ である．

定理 4.10 ([HM07]). 上記の記号の下で，$a,b \in M$, $(a \neq b, a\cdot b \neq 0)$ に対して，生成的多項式 X^3+sX+s の部分体問題の解は $H(a,b;X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型によって定理 4.5 の表 1 のように与えられる．特に，X^3+aX+a と X^3+bX+b の 2 つの M 上の最小分解体が一致するためには，次の条件を満たす $u \in M$ が存在することが必要十分である：

$$b = \frac{a(u^2+9u-3a)^3}{(u^3-2au^2-9au-2a^2-27a)^2}.$$

注意 4.11. Komatsu [Ko] は，char $k \neq 2,3$ の仮定の下で，3次生成的多項式 $g(t,Y) = Y^3 - t(Y+1) \in k(t)[Y]$ を取り扱っている．$\mathrm{Spl}_{k(t_1,t_2)}P(t_1,t_2;Z) = \mathrm{Spl}_{k(t_1,t_2)}g(t_1,Y) \cdot \mathrm{Spl}_{k(t_1,t_2)}g(t_2,Y)$ を満たす6次式 $P(t_1,t_2;Z)$ を，降下クンマー理論 ([Ko04] も参照) によって構成し，$P(t_1,t_2;Z)$ を用いて $g(t,Y)$ の部分体問題の解を与えている．

4.4 char $k = 3$ の場合

この小節では，char $k = 3$ の場合を取り扱う．この場合，

$$A_{\mathbf{s}} = s_1^2, \quad B_{\mathbf{s}} = -s_1^3, \quad D_{\mathbf{s}} = s_1^2 s_2^2 - s_2^3 - s_1^3 s_3$$

となる．式 (13) の X に関する係数を比較する事によって，

$$u_0 = \frac{s_2 t_1^2 - s_1^2 t_2 - s_2 t_1 (s_1^2 - s_2) u_2 - D_{\mathbf{s}} u_2^2}{s_1^2 t_1}, \tag{26}$$
$$u_1 = \frac{t_1 - (s_1^2 + s_2) u_2}{s_1}$$

が得られる．さらに $F_2(\mathbf{s},\mathbf{t};X)$ は

$$F_2(\mathbf{s},\mathbf{t};X) = X^6 + \frac{s_1^2 t_1^2}{D_{\mathbf{s}}} X^4 - \frac{t_1^3}{D_{\mathbf{s}}} X^3 + \frac{s_1^4 t_1^4}{D_{\mathbf{s}}^2} X^2 + \frac{s_1^2 t_1^5}{D_{\mathbf{s}}^2} X + \frac{t_1^6 D_{\mathbf{s}} - s_1^6 D_{\mathbf{t}}}{D_{\mathbf{s}}^3}$$

で与えられる．また $F_2(\mathbf{s},\mathbf{t};X)$ の X に関する判別式は

$$D_{\mathbf{s},\mathbf{t}} = \frac{B_{\mathbf{s}}^6 D_{\mathbf{t}}^3 (A_{\mathbf{s}}^3 B_{\mathbf{t}}^2 - 27 A_{\mathbf{t}}^3 D_{\mathbf{s}})^2}{D_{\mathbf{s}}^{15}} = \frac{s_1^{18} D_{\mathbf{t}}^3 (s_1^6 t_1^6)^2}{D_{\mathbf{s}}^{15}} = \frac{s_1^{30} t_1^{12} D_{\mathbf{t}}^3}{D_{\mathbf{s}}^{15}}$$

である．

定理 4.12. 条件 $a_1 b_1 \neq 0$ を満たす $\mathbf{a} = (a_1,a_2,a_3), \mathbf{b} = (b_1,b_2,b_3) \in M^3$ に対して，生成的多項式 $X^3 - s_1 X^2 + s_2 X - s_3$ の部分体問題の解は $F_2(\mathbf{a},\mathbf{b};X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型によって定理 4.5 の表 1 のように与えられる．

次に $a_1 = 0$ の場合を考察する．多項式 $f_3(0,s,-s) = X^3 + sX + s$ は，$\mathfrak{S}_3$ に対する k-生成的であるので，一般性を失うことなく $a_1 = 0, b_1 = 0$ であると仮定してよい．実際 $f_3(\mathbf{s};X) = X^3 - s_1 X^2 + s_2 X - s_3 = 0$ に対して

$$Y = \frac{s_1^2}{-s_2 - s_1 X}$$

と置けば

$$Y^3 + \frac{-s_1^6}{s_1^2 s_2^2 - s_2^3 - s_1^3 s_3} Y + \frac{-s_1^6}{s_1^2 s_2^2 - s_2^3 - s_1^3 s_3} = 0$$

が得られる．よって，$a_1 \cdot D_{\mathbf{a}} \neq 0$ を満たす $\mathbf{a} = (a_1,a_2,a_3) \in M^3$ に対して，多項式 $f_3(\mathbf{a};X)$ と

$$X^3 + \frac{-a_1^6}{a_1^2 a_2^2 - a_2^3 - a_1^3 a_3} X + \frac{-a_1^6}{a_1^2 a_2^2 - a_2^3 - a_1^3 a_3}$$

は M 上チルンハウス同値である．

変数の特殊化 $(s_1,t_1)=(0,0)$ を行い，式 (13) の X に関する係数を比較することで，

$$u_1=\frac{s_2(t_3-t_2u_0-u_0^3)}{s_3t_2},\quad u_2=0$$

が確認される．式 (23), (24), (25) は char $k=3$ に対しても成立し，

$$\begin{aligned}F_0(0,s_2,s_3,0,t_2,t_3;X) &= X^6-t_2X^4+t_3X^3+t_2^2X^2+t_2t_3X+\frac{s_2^3t_3^2-s_3^2t_2^3}{s_2^3},\\ F_1(0,s_2,s_3,0,t_2,t_3;X) &= \Big(X^2-\frac{t_2}{s_2}\Big)^3,\\ F_2(0,s_2,s_3,0,t_2,t_3;X) &= X^6\end{aligned}$$

となる．また $f_3(0,s,-s;X)=X^3+sX+s$ に対し，$\mathrm{Disc}_X f_3(0,s,-s;X)=-s^3$ である．ここで

$$\begin{aligned}G_0(s,t;X) &:= F_0(0,s,-s,0,t,-t)\\ &= X^6-tX^4-tX^3+t^2X^2-t^2X+\frac{t^2(s-t)}{s}\end{aligned}$$

と定義する；$\mathrm{Disc}_X G_0(s,t;X)=t^{15}/s^3$ である．

命題 4.13.　$G_0(s,t;X)$ は $\mathfrak{S}_3\times\mathfrak{S}_3$ に対する k-生成的多項式である．

定理 4.14.　条件 $ab\neq 0$ を満たす $a,b\in M$ に対して，生成的多項式 X^3+sX+s の部分体問題の解は $G_0(a,b;X)$ の M 上での既約因子 $h_\mu(X)$ への分解の型によって定理 4.5 の表 1 のように与えられる．

§5.　3 次巡回多項式の場合

巡回置換 $\sigma=(123)\in\mathfrak{S}_3$ は体 $k(x_1,x_2,x_3)$ に変数の置換

$$\sigma\ :\ x_1\longmapsto x_2,\ x_2\longmapsto x_3,\ x_3\longmapsto x_1$$

として作用しているとする．また，

$$z_1:=\frac{x_1-x_2}{x_2-x_3},\quad z_2:=\frac{x_2-x_3}{x_3-x_1},\quad z_3:=\frac{x_3-x_1}{x_1-x_2}$$

と置くと，

$$z_2=\frac{-1}{1+z_1},\quad z_3=\frac{-(1+z_1)}{z_1}$$

が得られる．さらに $K_1:=k(z_1,z_2,z_3)$ と置くと $K_1\subset k(x_1,x_2,x_3)$ であり，K_1 の k 上の超越次数は 1 である．また $C_3=\langle\sigma\rangle$ は体 $K_1=k(z_1)$ に

$$\sigma\ :\ z_1\longmapsto\frac{-1}{1+z_1}\longmapsto\frac{-(1+z_1)}{z_1}\longmapsto z_1$$

として忠実に作用する．そこで C_3-拡大 $K_1/K_1^{C_3}$ を考察するために，次の多項式 $g^{C_3}(\widetilde{m};X)$ を導入する：

$$g^{C_3}(\widetilde{m};X) := \prod_{x\in \mathrm{Orb}_{\langle\sigma\rangle}(z_1)} (X-x) = \Big(X-z_1\Big)\Big(X+\frac{1}{1+z_1}\Big)\Big(X+\frac{1+z_1}{z_1}\Big)$$
$$= X^3 - \widetilde{m}X^2 - (\widetilde{m}+3)X - 1,$$

$$\widetilde{m} = \frac{z_1^3-3z_1-1}{z_1(z_1+1)} = \frac{-(x_1^3+x_2^3+x_3^3-3x_1^2x_2-3x_2^2x_3-3x_3^2x_1+6x_1x_2x_3)}{(x_2-x_1)(x_3-x_1)(x_3-x_2)}.$$

このとき，$K_1^{C_3}=k(\widetilde{m})$ であり，さらに $g^{C_3}(\widetilde{m};X)$ の $k(\widetilde{m})$ 上の最小分解体は K_1 である．

補題 5.1.　多項式 $f_3(\mathbf{s};X)=X^3-s_1X^2+s_2X-s_3$ と $g^{C_3}(\widetilde{m};X)=X^3-\widetilde{m}X^2-(\widetilde{m}+3)X-1$ は体 $k(x_1,x_2,x_3)^{C_3}$ 上でチルンハウス同値である．

証明.　多項式 $g^{C_3}(\widetilde{m};X)$ の $k(x_1,x_2,x_3)^{C_3}$ 上の最小分解体は $k(x_1,x_2,x_3)$ であることが次の様に分かる．

(i) char $k\neq 2$ の場合：$k(x_1,x_2,x_3)^{C_3}=k(s_1,s_2,s_3,\Delta_{\mathbf{s}})$，但し $\Delta_{\mathbf{s}}=(x_2-x_1)(x_3-x_1)(x_3-x_2)$ である．更には，$i=1,2,3$ に対して

$$x_i = \frac{-\Delta_{\mathbf{s}}+s_1s_2-9s_3-2\Delta_{\mathbf{s}}z_i}{2(s_1^2-3s_2)},\quad z_i = -\frac{\Delta_{\mathbf{s}}-s_1s_2+9s_3}{2\Delta_{\mathbf{s}}} - \frac{(s_1^2-3s_2)x_i}{\Delta_{\mathbf{s}}} \tag{27}$$

が成り立つ．

(ii) char $k=2$ の場合：$k(x_1,x_2,x_3)^{C_3}=k(s_1,s_2,s_3,\beta_{\mathbf{s}})$，但し $\beta_{\mathbf{s}}$ は式 (11) によって与えられた Berlekamp の判別式である．整数 $i=1,2,3$ に対して，

$$x_i = \frac{(s_1s_2+s_3)(\beta_{\mathbf{s}}+z_i)}{s_1^2+s_2},\quad z_i = \beta_{\mathbf{s}} + \frac{(s_1^2+s_2)x_i}{s_1s_2+s_3}$$

が成り立つ．　□

ここで，$\widetilde{m}$ を s_1,s_2,s_3 と $\Delta_{\mathbf{s}}$ (char $k=2$ のときには $\beta_{\mathbf{s}}$) によって記述することを考える．任意の体 k 上において

$$k(x_1,x_2,x_3)^{C_3} = k(s_1,s_2,s_3,x_1x_2^2+x_2x_3^2+x_3x_1^2)$$

および

$$\widetilde{m} = \frac{-s_1^3+6s_1s_2-18s_3-3(x_1x_2^2+x_1^2x_3+x_2x_3^2)}{-s_1s_2+3s_3+2(x_1x_2^2+x_1^2x_3+x_2x_3^2)}$$

が成り立つ．よって char $k\neq 2$ の場合には，

$$x_1x_2^2+x_2x_3^2+x_3x_1^2 = (\Delta_{\mathbf{s}}+s_1s_2-3s_3)/2$$

となり，さらに

$$\widetilde{m} = -\frac{3\Delta_{\mathbf{s}} + 2s_1^3 - 9s_1s_2 + 27s_3}{2\Delta_{\mathbf{s}}} \quad \Big(= -\frac{3\Delta_{\mathbf{s}} + B_{\mathbf{s}}}{2\Delta_{\mathbf{s}}}\Big)$$

が成り立つ．また char $k = 2$ の場合は

$$x_1x_2^2 + x_2x_3^2 + x_3x_1^2 = s_1s_2 + \beta_{\mathbf{s}}s_1s_2 + \beta_{\mathbf{s}}s_3$$

であり，これより

$$\widetilde{m} = \frac{s_1^3 + s_1s_2 + \beta_{\mathbf{s}}s_1s_2 + \beta_{\mathbf{s}}s_3}{s_1s_2 + s_3} \quad \Big(= \frac{s_1A_{\mathbf{s}} + \beta_{\mathbf{s}}B_{\mathbf{s}}}{B_{\mathbf{s}}}\Big)$$

が得られる．

定理 4.5 を $M = k(x_1, x_2, x_3)^{C_3}$ に対して用いると，$f_3(\mathbf{s}; X)$ から $g^{C_3}(\widetilde{m}; X)$ への $k(x_1, x_2, x_3)^{C_3}$ 上で定義されたチルンハウス変換が 3 つ存在することが分かる．多項式 $F_2(\mathbf{s}, \mathbf{t}; X)$ の変数の特殊化 $(t_1, t_2, t_3) \mapsto (\widetilde{m}, -(\widetilde{m}+3), 1) \in k(x_1, x_2, x_3)^{C_3}$ によって，$f_3(\mathbf{s}; X)$ から $g^{C_3}(\widetilde{m}; X)$ への $k(x_1, x_2, x_3)^{C_3}$ 上のチルンハウス変換の係数 (c_0^g, c_1^g, c_2^g) を具体的に求めることができる：

$$g^{C_3}(\widetilde{m}; X) = \mathrm{Resultant}_Y\big(f_3(\mathbf{s}; Y), X - (c_0^g + c_1^gY + c_2^gY^2)\big).$$

まず char $k \neq 2$ の場合には，式 (17) から $F_2(\mathbf{s}, \widetilde{m}, -(\widetilde{m}+3), 1; X)$ の具体的な因数分解

$$\begin{aligned} &F_2(s_1, s_2, s_3, \widetilde{m}, -(\widetilde{m}+3), 1; X) \\ &= X\Big(X - \frac{A_{\mathbf{s}}^2}{\Delta_{\mathbf{s}}^2}\Big)\Big(X + \frac{A_{\mathbf{s}}^2}{\Delta_{\mathbf{s}}^2}\Big)\Big(X^3 - \frac{A_{\mathbf{s}}^4}{\Delta_{\mathbf{s}}^4}X - \frac{A_{\mathbf{s}}^3(2A_{\mathbf{s}}s_1 - 3s_1s_2 + 27s_3)}{\Delta_{\mathbf{s}}^5}\Big) \end{aligned}$$

が得られる．よって $\{c_2^g \mid \overline{g} = \overline{(1,\tau)} \in H\backslash G_{\mathbf{s},\mathbf{t}},\ \psi(\tau) \in \mathfrak{A}_3\} = \{0, A_{\mathbf{s}}^2/\Delta_{\mathbf{s}}^2, -A_{\mathbf{s}}^2/\Delta_{\mathbf{s}}^2\}$ となる．また，式 (27) から $c_2 = 0$ を得る．さらに式 (20) と (21) によって，c_2^g の値から c_0^g, c_1^g が次のように計算できる：

$$\begin{aligned} &(c_0, c_1, c_2) = \Big(\frac{E_{\mathbf{s}} - \Delta_{\mathbf{s}}}{2\Delta_{\mathbf{s}}}, -\frac{A_{\mathbf{s}}}{\Delta_{\mathbf{s}}}, 0\Big), \\ &(c_0^{g_1}, c_1^{g_1}, c_2^{g_1}) = \\ &\Big(\frac{A_{\mathbf{s}}(A_{\mathbf{s}}s_2 - s_2^2 + 3s_1s_3) - (A_{\mathbf{s}}s_1 - E_{\mathbf{s}})\Delta_{\mathbf{s}} - \Delta_{\mathbf{s}}^2}{2\Delta_{\mathbf{s}}^2}, \frac{A_{\mathbf{s}}(-2A_{\mathbf{s}}s_1 + E_{\mathbf{s}} + \Delta_{\mathbf{s}})}{2\Delta_{\mathbf{s}}^2}, \frac{A_{\mathbf{s}}^2}{\Delta_{\mathbf{s}}^2}\Big), \\ &(c_0^{g_2}, c_1^{g_2}, c_2^{g_2}) = \\ &\Big(\frac{-A_{\mathbf{s}}(A_{\mathbf{s}}s_2 - s_2^2 + 3s_1s_3) - (A_{\mathbf{s}}s_1 - E_{\mathbf{s}})\Delta_{\mathbf{s}} - \Delta_{\mathbf{s}}^2}{2\Delta_{\mathbf{s}}^2}, \frac{A_{\mathbf{s}}(2A_{\mathbf{s}}s_1 - E_{\mathbf{s}} + \Delta_{\mathbf{s}})}{2\Delta_{\mathbf{s}}^2}, -\frac{A_{\mathbf{s}}^2}{\Delta_{\mathbf{s}}^2}\Big), \end{aligned}$$

但し $E_{\mathbf{s}} = s_1s_2 - 9s_3$, $\overline{g_i} = \overline{(1,\tau_i)} \in H\backslash G_{\mathbf{s},\mathbf{t}}$, $\psi(\tau_i) \in \mathfrak{A}_3\backslash\{1\}$, $(i = 1, 2)$. 計算代数を使って，直接

$$z_2 = \frac{x_2 - x_3}{x_3 - x_1} = c_0^{g_1} + c_1^{g_1}x_1 + c_2^{g_1}x_1^2, \quad z_3 = \frac{x_3 - x_1}{x_1 - x_2} = c_0^{g_2} + c_1^{g_2}x_1 + c_2^{g_2}x_1^2 \tag{28}$$

であることが確認でき，これより $\psi(\tau_1) = (123) \in \mathfrak{A}_3$ かつ $\psi(\tau_2) = (132) \in \mathfrak{A}_3$ が得られる．

他方，char $k = 2$ の場合には，$A_{\mathbf{s}}^3B_{\mathbf{t}}^2 - 27A_{\mathbf{t}}^3D_{\mathbf{s}} = 0$，但し $\mathbf{t} = (t_1, t_2, t_3) = (\widetilde{m}, -(\widetilde{m}+3), 1)$，となる．よって補題 4.2 (1) により

$$F_2(s_1,s_2,s_3,\widetilde{m},-(\widetilde{m}+3),1;X)$$
$$=X\Big(X+\frac{(s_1^2+s_2)^2}{(s_1s_2+s_3)^2}\Big)^2\Big(X^3+\frac{(s_1^2+s_2)^4}{(s_1s_2+s_3)^4}X+\frac{(s_1^2+s_2)^3}{(s_1s_2+s_3)^4}\Big)$$

が得られる．式 (20) と (21) によって

$$(c_0,c_1,c_2)=\Big(\beta_{\mathbf{s}},\frac{s_1^2+s_2}{s_1s_2+s_3},0\Big)$$

を求めることができ，その他，式 (28) を満たすあと 2 つのチルンハウス変換の係数も

$$(c_0^{g1},c_1^{g1},c_2^{g1})=$$
$$\Big(\frac{\beta_{\mathbf{s}}(s_1^3+s_3)}{s_1s_2+s_3},\frac{(s_1^2+s_2)(s_1^3+s_3+\beta_{\mathbf{s}}s_1s_2+\beta_{\mathbf{s}}s_3)}{(s_1s_2+s_3)^2},\frac{(s_1^2+s_2)^2}{(s_1s_2+s_3)^2}\Big),$$
$$(c_0^{g2},c_1^{g2},c_2^{g2})=$$
$$\Big(\frac{s_1^3+s_1s_2+\beta_{\mathbf{s}}s_1^3+\beta_{\mathbf{s}}s_3}{s_1s_2+s_3},\frac{(s_1^2+s_2)(s_1^3+s_1s_2+\beta_{\mathbf{s}}s_1s_2+\beta_{\mathbf{s}}s_3)}{(s_1s_2+s_3)^2},\frac{(s_1^2+s_2)^2}{(s_1s_2+s_3)^2}\Big)$$

として得られる．

ここで $f_3(\mathbf{a};X)=X^3-a_1X^2+a_2X-a_3$ の M 上のガロア群は C_3 と同型であると仮定する．補題 5.1 において，変数の特殊化 $\mathbf{s}=(s_1,s_2,s_3)\mapsto\mathbf{a}=(a_1,a_2,a_3)\in M^3$，(但し $A_{\mathbf{a}}\neq 0$, $B_{\mathbf{a}}\neq 0$ とする)，を行うことで，$f_3(\mathbf{a};X)$ と $g^{C_3}(m;X)=X^3-mX^2-(m+3)X-1$ は M 上でチルンハウス同値となる．そのとき m は次のように与えられる：

$$m=\begin{cases}-\dfrac{3\Delta_{\mathbf{a}}+2a_1^3-9a_1a_2+27a_3}{2\Delta_{\mathbf{a}}}, & \text{char } k\neq 2 \text{ のとき},\\[2ex] \dfrac{a_1^3+a_1a_2+\beta_{\mathbf{a}}a_1a_2+\beta_{\mathbf{a}}a_3}{a_1a_2+a_3}, & \text{char } k=2 \text{ のとき}.\end{cases}\tag{29}$$

以下，$\mathbf{a}=(m,-(m+3),1),\mathbf{b}=(n,-(n+3),1)$ とすると，$f_3(\mathbf{a};X)=X^3-mX^2-(m+3)X-1$, $f_3(\mathbf{b};X)=X^3-nX^2-(n+3)X-1$ および

$$D_{\mathbf{a}}=\mathrm{Disc}_X f_3(\mathbf{a};X)=(m^2+3m+9)^2,$$
$$A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=D_{\mathbf{a}}D_{\mathbf{b}}(2mn+3m+3n+18)(2mn+3m+3n-9)$$

が得られる．また $\Delta_{\mathbf{a}}=m^2+3m+9$, $\Delta_{\mathbf{b}}=n^2+3n+9$ および

$$F_2(\mathbf{a},\mathbf{b};X)=F_2^+(m,n;X)F_2^-(m,n;X),$$

$$F_2^+(m,n;X)=X^3-\frac{\Delta_{\mathbf{b}}}{\Delta_{\mathbf{a}}}X-\frac{(m-n)\Delta_{\mathbf{b}}}{\Delta_{\mathbf{a}}^2},$$
$$F_2^-(m,n;X)=X^3-\frac{\Delta_{\mathbf{b}}}{\Delta_{\mathbf{a}}}X+\frac{(m+n+3)\Delta_{\mathbf{b}}}{\Delta_{\mathbf{a}}^2}$$

かつ

$$\mathrm{Disc}_X(F_2^+(m,n;X)) = \frac{\Delta_{\mathbf{b}}^2(2mn+3m+3n+18)^2}{\Delta_{\mathbf{a}}^4},$$
$$\mathrm{Disc}_X(F_2^-(m,n;X)) = \frac{\Delta_{\mathbf{b}}^2(2mn+3m+3n-9)^2}{\Delta_{\mathbf{a}}^4}$$

となることが分かる．ここで $F_2^-(m,n;X) = F_2^+(m,-n-3;X)$ に注意しておく．もし $m+n+3=0$ であれば，$X^3-mX^2-(m+3)X-1$ と $X^3-nX^2-(n+3)X-1$ は M 上で同じ最小分解体をもつ．これより

$$X^3-mX^2-(m+3)X-1 \quad と \quad X^3+(m+3)X^2+mX-1$$

は M 上でチルンハウス同値である．もし $(2mn+3m+3n+18)(2mn+3m+3n-9)=0$ であれば，定理 4.3 (1) から，$X^3-mX^2-(m+3)X-1$ と $X^3-nX^2-(n+3)X-1$ は M 上で同じ最小分解体をもつ．

定理 5.2. 条件

$$(2mn+3m+3n+18)(2mn+3m+3n-9) \neq 0$$

を満たす $m,n \in M$ に対して，2 つの多項式 $X^3-mX^2-(m+3)X-1$ と $X^3-nX^2-(n+3)X-1$ の M 上の最小分解体が一致するためには，$F_2^+(m,n;X)F_2^-(m,n;X)$ が M 内に根を持つことが必要十分である．

例 5.3. $M=\mathbb{Q}$ とする．もし $(m,n) \in \{(-1,5),(-1,1259),(0,54),(5,1259)\}$ であれば $F_2^+(m,n;X)$ は $\mathbb{Q}$ 上 1 次因子 3 つに完全分解する．もし $(m,n) \in \{(-1,12),(0,3),(1,66),(2,2389),(3,54),(5,12),(12,1259)\}$ であれば $F_2^-(m,n;X)$ は $\mathbb{Q}$ 上 1 次因子 3 つに完全分解する．よって

$$L_{-1}=L_5=L_{12}=L_{1259}, \quad L_0=L_3=L_{54}, \quad L_1=L_{66}, \quad L_2=L_{2389}$$

を得る．但し，$L_m = \mathrm{Spl}_{\mathbb{Q}}(X^3-mX^2-(m+3)X-1)$．我々は計算機を用いることによって，$-1 \leq m < n \leq 100000$ の範囲の整数 m, n については，$F_2^+(m,n;X)F_2^-(m,n;X)$ が $\mathbb{Q}$ 内に一次因子を持つのは，上記の (m,n) に限られることを確認している．

もし $\mathrm{char}\, k \neq 2,3$ であれば，式 (29) を用いることによって，$F_2^+(m,n;X)$ と

$$g^+(m,n;X) := X^3 + \frac{3(mn+6m-3n+9)}{2mn+3m+3n+18}X^2 - \frac{3(mn-3m+6n+9)}{2mn+3m+3n+18}X - 1$$

は M 上でチルンハウス同値であることが分かる．また，同様にして $F_2^-(m,n;X)$ と

$$g^-(m,n;X) := X^3 + \frac{3(mn-3m-3n-18)}{2mn+3m+3n-9}X^2 - \frac{3(mn+6m+6n+9)}{2mn+3m+3n-9}X - 1$$

は M 上でチルンハウス同値であることが分かる．

今，$Z=(X-1)/(X+2)$ とすると，$X=-(2Z+1)/(Z-1)$ であり，

$$\begin{aligned} h^+(m,n;Z) &:= \frac{1}{3^3(m-n)}\,g^+\Big(m,n;\frac{-(2Z+1)}{Z-1}\Big)\\ &= Z^3-\frac{mn+3n+9}{m-n}Z^2-\frac{mn+3m+9}{m-n}Z-1,\\ h^-(m,n;Z) &:= \frac{-1}{3^3(m+n+3)}\,g^-\Big(m,n;\frac{-(2Z+1)}{Z-1}\Big)\\ &= Z^3+\frac{mn+3m+3n}{m+n+3}Z^2+\frac{mn-9}{m+n+3}Z-1 \end{aligned}$$

が成り立つ．また

$$\mathrm{Disc}_Z(h^+(m,n;Z))=\frac{\Delta_{\mathbf{a}}^2\Delta_{\mathbf{b}}^2}{(m-n)^4},\quad \mathrm{Disc}_Z(h^-(m,n;Z))=\frac{\Delta_{\mathbf{a}}^2\Delta_{\mathbf{b}}^2}{(m+n+3)^4}$$

を得る．

他方，char $k=3$ の場合には，小節 4.4 の結果を用いて，$F_2^+(m,n;X)$ と $h^+(m,n;Z)$，ならびに，$F_2^-(m,n;X)$ と $h^-(m,n;Z)$ がそれぞれ M 上でチルンハウス同値であることを直接に確認できる．よって Morton [Mor94], Chapman [Cha96] の結果の類似として，次の定理が得られる．

定理 5.4.　体 k の標数は 2 ではないと仮定する．また，$m,n\in M$ に対して

$$(m-n)(m+n+3)(2mn+3m+3n+18)(2mn+3m+3n-9)\neq 0$$

とする．このとき，2 つの多項式 $X^3-mX^2-(m+3)X-1$ と $X^3-nX^2-(n+3)X-1$ の M 上の最小分解体が一致するためには，次の条件を満たす $z\in M$ が存在することが必要十分である：

$$n=\frac{m(z^3-3z-1)-9z(z+1)}{mz(z+1)+z^3+3z^2-1}\ \text{または}\ n=-\frac{m(z^3+3z^2-1)+3(z^3-3z-1)}{mz(z+1)+z^3+3z^2-1}.$$

§6. 幾つかの 6 次生成的多項式

まず char $k\neq 3$ とする．また H_1, H_2 を $\mathfrak{S}_3$ の部分群，$k(s,t)$ を k 上 2 変数有理関数体とする．群 H_1 に対する，1 パラメータ s 付きの k-生成的多項式 $f_3(\mathbf{a};X)\in k(s)[X]$ と，群 H_2 に対する，1 パラメータ t 付きの k-生成的多項式 $f_3(\mathbf{b};X)\in k(t)[X]$ を用意する ($\mathbf{a}\in k(s)^3$, $\mathbf{b}\in k(t)^3$)．また，多項式 $g^{(H_1,H_2)}(s,t;X):=F_2(\mathbf{a},\mathbf{b};X)$ は重根を持たないと仮定する．このとき，定理 3.10 より $g^{(H_1,H_2)}(s,t;X)$ は $H_1\times H_2$ に対する 2 つのパラメータ s,t 付きの k-生成的多項式となる．ここで，1 パラメータの $\mathbb{Q}$-生成的多項式は群 $\{1\},C_2,C_3,\mathfrak{S}_3$ に対するものを除けば，存在しないことに注意しておく (cf. [BR97], [Le07], [CHKZ])．さて，$(H_1,H_2)\in\{(\mathfrak{S}_3,\mathfrak{S}_3),(\mathfrak{S}_3,C_3),(\mathfrak{S}_3,C_2),(\mathfrak{S}_3,\{1\}),(C_3,C_2)\}$ とする．このとき，$L_{\mathbf{a}}\cap L_{\mathbf{b}}=k(s,t)$ であり，定理 4.5 から，$g^{(H_1,H_2)}(s,t;X)$ は $k(s,t)$ 上で既約になる．したがって，このとき $H_1\times H_2$ は自然に $\mathfrak{S}_6$ の可移部分群と見なすことができる．

(1) $(H_1, H_2) = (\mathfrak{S}_3, \mathfrak{S}_3)$ の場合：$\mathbf{a} = (0, s, -s)$, $\mathbf{b} = (0, t, -t)$ とすると，$f_3(\mathbf{a}; X) = X^3 + sX + s$, $f_3(\mathbf{b}; X) = X^3 + tX + t$, $A_{\mathbf{a}}^3 B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3 D_{\mathbf{a}} = -729s^2t^2(4st + 27s + 27t)$ であり，

$$\begin{aligned} g^{(\mathfrak{S}_3, \mathfrak{S}_3)}(s, t; X) &:= \frac{1}{3^6} F_2(0, s, -s, 0, t, -t; 3X) \\ &= X^6 + \frac{2t}{s(4s+27)} X^4 + \frac{t}{s^2(4s+27)} X^3 \\ &\quad + \frac{t^2}{s^2(4s+27)^2} X^2 + \frac{t^2}{s^3(4s+27)^2} X + \frac{(s-t)t^2}{s^4(4s+27)^3} \end{aligned}$$

は $\mathfrak{S}_3 \times \mathfrak{S}_3$ に対する k-生成的多項式である．

(2) $(H_1, H_2) = (\mathfrak{S}_3, C_3)$ の場合：$\mathbf{a} = (0, s, -s)$, $\mathbf{b} = (t, -t-3, 1)$ とすれば，$f_3(\mathbf{a}; X) = X^3 + sX + s$, $f_3(\mathbf{b}; X) = X^3 - tX^2 - (t+3)X - 1$, $A_{\mathbf{a}}^3 B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3 D_{\mathbf{a}} = 729s^2(t^2+3t+9)^2(t^2+3t+9+s)$ を得る．このとき，

$$\begin{aligned} g^{(\mathfrak{S}_3, C_3)}(s, t; X) &:= F_2(0, s, -s, t, -t-3, 1; X) \\ &= X^6 - \frac{6(t^2+3t+9)}{s(4s+27)} X^4 - \frac{(2t+3)(t^2+3t+9)}{s^2(4s+27)} X^3 \\ &\quad + \frac{9(t^2+3t+9)^2}{s^2(4s+27)^2} X^2 + \frac{3(2t+3)(t^2+3t+9)^2}{s^3(4s+27)^2} X \\ &\quad + \frac{(t^2+3t+9)^2(4st^2+27t^2+12st+9s+81t+243)}{s^4(4s+27)^3} \end{aligned}$$

は群 $\mathfrak{S}_3 \times C_3 \cong C_3 \wr C_2 \cong (C_3 \times C_3) \rtimes C_2$ に対する k-生成的多項式である．

さらに特殊化 $(s, t) \mapsto (a, b) \in M^2$ のとき，もし $b^2 + 3b + 9 + a = 0$ であれば $X^3 + aX + a$ と $X^3 - bX^2 - (b+3)X - 1$ は M 上で同じ最小分解体を持つ．すなわち，

$$X^3 - (b^2+3b+9)X - (b^2+3b+9) \quad \text{と} \quad X^3 - bX^2 - (b+3)X - 1$$

は M 上でチルンハウス同値である．また，もし $4ab^2 + 27b^2 + 12ab + 9a + 81b + 243 = 0$ であれば $X^3 + aX + a$ と $X^3 - bX^2 - (b+3)X - 1$ は M 上で同じ最小分解体を持つ．よって

$$X^3 - \frac{27(b^2+3b+9)}{(2b+3)^2} X - \frac{27(b^2+3b+9)}{(2b+3)^2} \quad \text{と} \quad X^3 - bX^2 - (b+3)X - 1$$

は M 上でチルンハウス同値である．これは根のアフィン変換によって得られる．

(3) $(H_1, H_2) = (\mathfrak{S}_3, C_2)$ の場合：$\mathbf{a} = (0, s, -s)$, $\mathbf{b} = (0, -t, 0)$ とすると，$f_3(\mathbf{a}; X) = X^3 + sX + s$, $f_3(\mathbf{b}; X) = X(X^2 - t)$, $A_{\mathbf{a}}^3 B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3 D_{\mathbf{a}} = 729s^2t^3(4s+27)$ となる．このとき，

$$g^{(\mathfrak{S}_3, C_2)}(s, t; X) := \frac{1}{3^6} F_2(0, s, -s, 0, -t, 0; 3X)$$

$$= X^6 - \frac{2t}{s(4s+27)}X^4 + \frac{t^2}{s^2(4s+27)^2}X^2 + \frac{t^3}{s^4(4s+27)^3}$$

は $\mathfrak{S}_3 \times C_2 \cong D_6$ に対する k-生成的多項式である．但し D_6 は位数 12 の二面体群である．

(4) $(H_1, H_2) = (\mathfrak{S}_3, \{1\})$ の場合：更に，$\mathrm{char}\, k \neq 2$ を仮定する．この場合，$\mathbf{a} = (0, s, -s)$, $\mathbf{b} = (0, -1, 0)$ とすると，$f_3(\mathbf{a}; X) = X^3 + sX + s$, $f_3(\mathbf{b}; X) = X(X+1)(X-1)$, $A_{\mathbf{a}}^3 B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3 D_{\mathbf{a}} = 729s^2(4s+27)$. したがって，$\mathfrak{S}_3$ に対する k-生成的多項式

$$\begin{aligned} g^{(\mathfrak{S}_3, \{1\})}(s, t; X) &:= \frac{1}{3^6} F_2(0, s, -s, 0, -1, 0; 3X) \\ &= X^6 - \frac{2}{s(4s+27)}X^4 + \frac{1}{s^2(4s+27)^2}X^2 + \frac{1}{s^4(4s+27)^3} \end{aligned}$$

が得られる．更には，$\mathfrak{S}_3$ に対する 1 つのパラメータ s 付きの k-生成的多項式

$$\begin{aligned} h^{\mathfrak{S}_3}(s; X) &:= (s(4s+27))^6\, g^{(\mathfrak{S}_3, \{1\})}\Big(s, t; \frac{X}{s(4s+27)}\Big) \\ &= X^6 - 2s(4s+27)X^4 + s^2(4s+27)^2X^2 + s^2(4s+27)^3 \end{aligned}$$

が得られる．2 つの多項式 $f_3(\mathbf{a}; X) = X^3 + sX + s$ と $h^{\mathfrak{S}_3}(s; X)$ は $k(s)$ 上同じ最小分解体を持つ．

(5) $(H_1, H_2) = (C_3, C_2)$ の場合：$\mathbf{a} = (s, -s-3, 1)$, $\mathbf{b} = (0, -t, 0)$ とすると，$f_3(\mathbf{a}; X) = X^3 - sX^2 - (s+3)X - 1$, $f_3(\mathbf{b}; X) = X(X^2 - t)$, $A_{\mathbf{a}}^3 B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3 D_{\mathbf{a}} = -729t^3(s^2+3s+9)^2$ である．このとき，

$$\begin{aligned} g^{(C_3, C_2)}(s, t; X) &:= F_2(s, -s-3, 1, 0, -t, 0; X) \\ &= X^6 - \frac{6t}{s^2+3s+9}X^4 + \frac{9t^2}{(s^2+3s+9)^2}X^2 - \frac{(2s+3)^2t^3}{(s^2+3s+9)^4} \end{aligned}$$

は $C_3 \times C_2 \cong C_6$ に対する k-生成的多項式となる．

また，$\mathrm{char}\, k = 3$ の場合，小節 4.4 の結果から，多項式 $F_0(\mathbf{a}, \mathbf{b}; X)$ を $F_2(\mathbf{a}, \mathbf{b}; X)$ の代わりに用いなくてはならない．ここでは，各 (H_1, H_2) に対する多項式 $g^{(H_1, H_2)}(s, t; X) := F_0(\mathbf{a}, \mathbf{b}; X)$ の計算結果のみを記述しておく：

$$\begin{aligned} g^{(\mathfrak{S}_3, \mathfrak{S}_3)}(1/s, t; X) &= X^6 - tX^4 - tX^3 + t^2X^2 - t^2X - t^2(st-1), \\ g^{(\mathfrak{S}_3, C_3)}(1/s, t; X) &= X^6 + tX^5 + t(t+1)X^4 + (st^3 - t^2 + 1)X^3 \\ &\quad - t(st^3 - t + 1)X^2 - t(st^3+1)X + s^2t^6 + st^4 - st^3 + 1, \\ g^{(\mathfrak{S}_3, C_2)}(1/s, t; X) &= X^6 - tX^4 + t^2X^2 + st^3, \\ g^{(\mathfrak{S}_3, \{1\})}(1/s, t; X) &= X^6 - X^4 + X^2 + s, \\ g^{(C_3, C_2)}(1/s, t; X) &= X^6 + \frac{t^2}{s^4+s^2+1}X^2 + \frac{s^2t^3}{s^8+s^4+1}. \end{aligned}$$

参考文献

[Ber76] E. R. Berlekamp, *An analog to the discriminant over fields of characteristic two*, J. Algebra **38** (1976), 315–317.

[BJY86] A. A. Bruen, C. U. Jensen, N. Yui, *Polynomials with Frobenius groups of prime degree as Galois Groups II*, J. Number Theory **24** (1986), 305–359.

[BR97] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159–179.

[Cha96] R. J. Chapman, *Automorphism polynomials in cyclic cubic extensions*, J. Number Theory **61** (1996), 283–291.

[CHKZ] H. Chu, S. Hu, M. Kang, J. Zhang, *Groups with essential dimension one*, preprint. arXiv:math/0611917v1 [math.AG].

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[HH05-1] K. Hashimoto, A. Hoshi, *Families of cyclic polynomials obtained from geometric generalization of Gaussian period relations*, Math. Comp. **74**, 1519-1530 (2005).

[HH05-2] K. Hashimoto, A. Hoshi, *Geometric generalization of Gaussian period relations with application to Noether's problem for meta-cyclic groups*, Tokyo J. Math. **28** 13-32 (2005).

[HM99] K. Hashimoto, K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications, Dev. Math., 2, Doredrecht: Kluwer Acad. Publ. 165–181, 1999.

[HM07] A. Hoshi, K. Miyake, *Tschirnhausen transformation of a cubic generic polynomial and a 2-dimensional involutive Cremona transformation*, Proc. Japan Acad., Series A **83** (2007), 21–26.

[HM] A. Hoshi, K. Miyake, *A geometric framework for the subfield problem of generic polynomials via Tschirnhausen transformation*, preprint. arXiv:0710.0287v1 [math.NT] `http://arxiv.org/abs/0710.0287`

[Hup67] B. Huppert, *Endliche Gruppen. I.*, Grundlehren der Mathematischen Wissenschaften 134, Springer-Verlag, Berlin-New York 1967.

[JLY02] C. Jensen, A. Ledet, N. Yui, *Generic polynomials, constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, Cambridge, 2002.

[Kem96] G. Kemper, *A constructive approach to Noether's problem*, Manuscripta Math. **90** (1996), 343–363.

[Kem01] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), 139–141.

[KM00] G. Kemper, E. Mattig, *Generic polynomils with few parameters*, J. Symbolic Comput. **30** (2000), 843-857.

[Ki05] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), 427–447.

[Ki06] M. Kida, *Cyclic polynomials arising from Kummer theory of norm algebraic tori*, Algorithmic number theory, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 102–113, 2006.

[Ko04] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta math. **114** (2004), 265-279.

[Ko] T. Komatsu, *Generic sextic polynomial related to the subfield problem of a cubic polynomial*, preprint. `http://www.math.kyushu-u.ac.jp/coe/report/pdf/2006-9.pdf`

[Le07] A. Ledet, *On groups with essential dimension one*, J. Algebra, **311** (2007) 31–37.

[Miy99] K. Miyake, *Linear fractional transformations and cyclic polynomials*, Algebraic number theory (Hapcheon/Saga, 1996). Adv. Stud. Contemp. Math. (Pusan) 1 (1999), 137–142.

[Miy03] K. Miyake, *Some families of Mordell curves associated to cubic fields*, J. Comput. Appl. Math. **160** (2003), 217–231.

[Miy04] K. Miyake, *An introduction to elliptic curves and their Diophantine geometry—Mordell curves*, Ann. Sci. Math. Québec **28** (2004), 165–178.

[Miy06] K. Miyake, *Cubic fields and Mordell curves*, Number theory, 175–183, Dev. Math., 15, Springer, New York, 2006.

[Mor94] P. Morton, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory **49** (1994), 183–208.

[Sha74] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

Akinari HOSHI
Department of Mathematics
School of Education
Waseda University
1–6–1 Nishi-Waseda Shinjuku-ku
Tokyo, 169–8050, Japan
E-mail: hoshi@ruri.waseda.jp

Katsuya MIYAKE
Department of Mathematics
School of Fundamental Science and Engineering
Waseda University
3–4–1 Ohkubo Shinjuku-ku
Tokyo, 169–8555, Japan
E-mail: miyakek@aoni.waseda.jp