On the field intersection problem of generic polynomials: a survey

By

Akinari Hoshi* and Katsuya Miyake**

Abstract

Let k be a field of characteristic $\neq 2$. We survey a general method of the field intersection problem of generic polynomials via formal Tschirnhausen transformation. We announce some of our recent results of cubic, quartic and quintic cases the details of which are to appear elsewhere. In this note, we give an explicit answer to the problem in the cases of cubic and dihedral quintic by using multi-resolvent polynomials.

§ 1. Introduction

Let G be a finite group, k a field of characteristic $\neq 2$, M a field containing k with $\#M = \infty$, and $k(\mathbf{t})$ the rational function field over k with n indeterminates $\mathbf{t} = (t_1, \ldots, t_n)$. Our main interest in this note is a k-generic polynomial for G (cf. [DeM83], [Kem01], [JLY02]).

Definition. A polynomial $f_{\mathbf{t}}(X) \in k(\mathbf{t})[X]$ is called k-generic for G if it has the following property: the Galois group of $f_{\mathbf{t}}(X)$ over $k(\mathbf{t})$ is isomorphic to G and every G-Galois extension L/M over an arbitrary infinite field $M \supset k$ can be obtained as $L = \mathrm{Spl}_M f_{\mathbf{a}}(X)$, the splitting field of $f_{\mathbf{a}}(X)$ over M, for some $\mathbf{a} = (a_1, \ldots, a_n) \in M^n$.

Let $f_{\mathbf{t}}^G(X) \in k(\mathbf{t})[X]$ be a k-generic polynomial for G. Examples of k-generic polynomials for G are known for various pairs of (k, G) (for example, see [Kem94],

[KM00], [JLY02], [Rik04]). Since a k-generic polynomial $f_{\mathbf{t}}^G(X)$ for G covers all G-Galois extensions over $M \supset k$ by specializing parameters, it is natural to ask the following problem:

Field isomorphism problem of a generic polynomial. *For a field $M \supset k$ and $\mathbf{a}, \mathbf{b} \in M^n$, determine whether $\mathrm{Spl}_M f_{\mathbf{a}}^G(X)$ and $\mathrm{Spl}_M f_{\mathbf{b}}^G(X)$ are isomorphic over M or not.*

It would be desired to give an answer to the problem within the base field M by using the data $\mathbf{a}, \mathbf{b} \in M^n$. Throughout this paper, we assume that $f_{\mathbf{a}}^G(X)$ is separable for $\mathbf{a} \in M^n$.

Let S_n (resp. D_n, C_n) be the symmetric (resp. the dihedral, the cyclic) group of degree n. We take k-generic polynomials

$$f_t^{C_3}(X) := X^3 - tX^2 - (t+3)X - 1 \in k(t)[X],$$
$$f_t^{S_3}(X) := X^3 + tX + t \in k(t)[X],$$
$$f_{s,t}^{D_4}(X) := X^4 + sX^2 + t \in k(s,t)[X]$$

for $G = C_3$, S_3, D_4, respectively. By using formal Tschirnhausen transformation, we showed the following theorem which is an analogue to the results of Morton [Mor94] and Chapman [Cha96].

Theorem 1.1 ([Mor94], [Cha96], [HM]). *For $m, n \in M$, the splitting fields of $f_m^{C_3}(X)$ and of $f_n^{C_3}(X)$ over M coincide if and only if there exists $z \in M$ such that either*

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

We also have analogues to the above theorem for two non-abelian groups S_3 and D_4 via formal Tschirnhausen transformation.

Theorem 1.2 ([HM07]). *Assume that char $k \neq 3$. For $a, b \in M$ with $a \neq b$, the splitting fields of $f_a^{S_3}(X)$ and of $f_b^{S_3}(X)$ over M coincide if and only if there exists $u \in M$ such that*

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

Theorem 1.3 ([HM-2]). *For $a, b \in M$, we assume that $\mathrm{Gal}(f_{a,b}^{D_4}/M) = D_4$. Then for $a, b, a', b' \in M$, the splitting fields of $f_{a,b}^{D_4}(X)$ and of $f_{a',b'}^{D_4}(X)$ over M coincide if and only if there exist $p, q \in M$ such that either*

(i) $a' = ap^2 - 4bpq + abq^2$, $b' = b(p^2 - apq + bq^2)^2$ *or*

(ii) $a' = 2(ap^2 - 4bpq + abq^2)$, $b' = (a^2 - 4b)(p^2 - bq^2)^2$.

By applying Hilbert's irreducibility theorem (cf. for example [JLY02, Chapter 3]) and Siegel's theorem for curves of genus 0 (cf. for example [Lan78, Theorem 6.1]) to the theorems above respectively, we get the following corollaries:

Corollary 1.4. *Let $f_{\mathbf{a}}^G(X) = f_m^{C_3}(X)$ (resp. $f_a^{S_3}(X)$, $f_{a,b}^{D_4}(X)$) be as above in Theorem 1.1 (resp. Theorem 1.2, Theorem 1.3) with given $\mathbf{a} \in M^n$, and suppose that $M \supset k$ is Hilbertian (e.g. a number field). Then there exist infinitely many $\mathbf{b} \in M^n$ such that $\mathrm{Spl}_M f_{\mathbf{a}}^G(X) = \mathrm{Spl}_M f_{\mathbf{b}}^G(X)$.*

Corollary 1.5. *Let M be a number field and $\mathcal{O}_M$ the ring of integers in M. For $f_a^G(X) = f_m^{C_3}(X)$ (resp. $f_a^{S_3}(X)$) as above in Theorem 1.1 (resp. Theorem 1.2) with a given integer $a \in \mathcal{O}_M$, there exist only finitely many integers $b \in \mathcal{O}_M$ such that $\mathrm{Spl}_M f_a^G(X) = \mathrm{Spl}_M f_b^G(X)$.*

Indeed integers $b \in \mathcal{O}_M$ as in Corollary 1.5 are derived from some integer solutions of (finitely many) cubic Thue equations $aXY(X + Y) + X^3 + 3XY^2 - Y^3 = \lambda$ (resp. $X^3 - 2aX^2Y - 9aXY^2 - 2aY^3 - 27aY^3 = \lambda$) which are curves of genus 1 (see also the proof of [Lan78, Theorem 6.1]).

Kemper [Kem01], furthermore, showed that for a subgroup H of G every H-Galois extension over M is also given by a specialization $f_{\mathbf{a}}^G(X)$, $\mathbf{a} \in M^n$, of a generic polynomial $f_{\mathbf{t}}^G(X)$ for G. Hence a problem naturally arises.

Field intersection problem of a generic polynomial. *For a field $M \supset k$ and $\mathbf{a}, \mathbf{b} \in M^n$, determine the intersection of $\mathrm{Spl}_M f_{\mathbf{a}}^G(X)$ and $\mathrm{Spl}_M f_{\mathbf{b}}^G(X)$.*

Clearly if we get an answer to the field intersection problem of a k-generic polynomial, we also obtain an answer to the corresponding field isomorphism problem.

The aim of this note is to survey a method to give an answer to the isomorphism problem and the intersection problem of k-generic polynomials via formal Tschirnhausen transformation and multi-resolvent polynomials. In Section 2, we review known results about resolvent polynomials. In Section 3, we recall a formal Tschirnhausen transformation which is given in [HM]. In Section 4, we give a general method to solve the intersection problem of k-generic polynomials. In Section 5, we obtain an explicit answer to the problems in the cubic case. We give a proof of Theorem 1.2 as a special case of the intersection problem of $f_t^{S_3}(X) = X^3 + tX + t$ via formal Tschirnhausen transformation. In Section 6, we take the k-generic polynomial

$$f_{s,t}^{D_5}(X) = X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2 - t - 2s - 1)X^2 + sX + t \in k(s,t)[X]$$

for D_5 which is called Brumer's quintic (cf. [JLY02]). Based on the general result, we illustrate how to give an answer to the problem for $f_{s,t}^{D_5}(X)$ by multi-resolvent polynomials. We also give some numerical examples.

§2. Resolvent polynomials

In this section we review some known results in the computational aspects of Galois theory (cf. the text books [Coh93], [Ade01]). One of the fundamental tools in the determination of Galois group of a polynomial is resolvent polynomials; an absolute resolvent polynomial was introduced by Lagrange [Lag1770] and a relative one by Stauduhar [Sta73]. Several kinds of methods to compute resolvent polynomials have been developed by many mathematicians (see, for example, [Sta73], [Gir83], [SM85], [Yok97], [MM97], [AV00], [GK00] and the references therein).

Let $M(\supset k)$ be an infinite field and $\overline{M}$ a fixed algebraic closure of M. Let $f(X) := \prod_{i=1}^{m}(X - \alpha_i) \in M[X]$ be a separable polynomial of degree m with some fixed order of the roots $\alpha_1, \ldots, \alpha_m \in \overline{M}$. The Galois group of the splitting field $\mathrm{Spl}_M f(X)$ of $f(X)$ over M may be obtained by using suitable resolvent polynomials.

Let $k[\mathbf{x}] := k[x_1, \ldots, x_m]$ be the polynomial ring over k with m indeterminates $x_1, \ldots, x_m$. Put $R := k[\mathbf{x}, 1/\Delta_{\mathbf{x}}]$, where $\Delta_{\mathbf{x}} := \prod_{1 \leq i < j \leq m}(x_j - x_i)$. We take a surjective evaluation homomorphism $\omega_f : R \to k(\alpha_1, \ldots, \alpha_m)$, $\Theta(x_1, \ldots, x_m) \mapsto \Theta(\alpha_1, \ldots, \alpha_m)$ for $\Theta \in R$. We note that $\omega_f(\Delta_{\mathbf{x}}) \neq 0$ from the assumption that $f(X)$ is separable. The kernel of the map ω_f is the ideal $I_f = \{\Theta(x_1, \ldots, x_m) \in R \mid \Theta(\alpha_1, \ldots, \alpha_m) = 0\}$.

Let S_m be the symmetric group of degree m. We extend the action of S_m on m letters $\{1, \ldots, m\}$ to that on R by $\pi(\Theta(x_1, \ldots, x_m)) := \Theta(x_{\pi(1)}, \ldots, x_{\pi(m)})$. We define the Galois group of a polynomial $f(X)$ over M by $\mathrm{Gal}(f/M) := \{\pi \in S_m \mid \pi(I_f) \subseteq I_f\}$. We write $\mathrm{Gal}(f) := \mathrm{Gal}(f/M)$ for simplicity. The Galois group of the splitting field $\mathrm{Spl}_M f(X)$ of the polynomial $f(X)$ over M is isomorphic to $\mathrm{Gal}(f)$. If we take another ordering of roots $\alpha_{\pi(1)}, \ldots, \alpha_{\pi(m)}$ of $f(X)$ for some $\pi \in S_m$, the corresponding realization of $\mathrm{Gal}(f)$ is conjugate in S_m. Hence, for arbitrary ordering of the roots of $f(X)$, $\mathrm{Gal}(f)$ is determined up to conjugacy in S_m.

Definition. For $H \leq G \leq S_m$, an element $\Theta \in R$ is called a G-primitive H-invariant if $H = \mathrm{Stab}_G(\Theta) := \{\pi \in G \mid \pi(\Theta) = \Theta\}$. For a G-primitive H-invariant Θ, the polynomial

$$\mathcal{RP}_{\Theta,G}(X) = \prod_{\overline{\pi} \in G/H}(X - \pi(\Theta)) \in R^G[X],$$

where $\overline{\pi}$ runs through the left cosets of H in G, is called the *formal G-relative H-invariant resolvent* by Θ, and the polynomial

$$\mathcal{RP}_{\Theta,G,f}(X) = \prod_{\overline{\pi} \in G/H}\left(X - \omega_f(\pi(\Theta))\right) \in M[X]$$

is called the *G-relative H-invariant resolvent of f by Θ*.

The following theorem is fundamental in the theory of resolvent polynomials (cf. for example [Ade01, p.95]).

Theorem 2.1.   *Let $H \leq G \leq S_m$ be a tower of finite groups and Θ a G-primitive H-invariant. Assume $\mathrm{Gal}(f) \leq G$. Suppose that $\mathcal{RP}_{\Theta,G,f}(X) = \prod_{i=1}^{l} h_i^{e_i}(X)$ gives the decomposition of $\mathcal{RP}_{\Theta,G,f}(X)$ into a product of powers of distinct irreducible polynomials $h_i(X), i = 1, \ldots, l$, in $M[X]$. Then we have a bijection*

$$
\begin{aligned}
\mathrm{Gal}(f) \backslash G / H &\longrightarrow \{h_1^{e_1}(X), \ldots, h_l^{e_l}(X)\} \\
\mathrm{Gal}(f)\,\pi\,H &\longmapsto h_\pi(X) = \prod_{\tau H \subseteq \mathrm{Gal}(f)\,\pi\,H} \big(X - \omega_f(\tau(\Theta))\big)
\end{aligned}
$$

where the product runs through the left cosets τH of H in G contained in $\mathrm{Gal}(f)\,\pi\,H$, that is, through $\tau = \pi_\sigma \pi$ where π_σ runs a system of representative of the left cosets of $\mathrm{Gal}(f) \cap \pi H \pi^{-1}$; each $h_\pi(X)$ is irreducible or a power of an irreducible polynomial with $\deg(h_\pi(X)) = |\mathrm{Gal}(f)\,\pi\,H|/|H| = |\mathrm{Gal}(f)|/|\mathrm{Gal}(f) \cap \pi H \pi^{-1}|$.

Corollary 2.2.   *If $\mathrm{Gal}(f) \leq \pi H \pi^{-1}$ for some $\pi \in G$ then $\mathcal{RP}_{\Theta,G,f}(X)$ has a linear factor over M. Conversely, if $\mathcal{RP}_{\Theta,G,f}(X)$ has a non-repeated linear factor over M then there exists $\pi \in G$ such that $\mathrm{Gal}(f) \leq \pi H \pi^{-1}$.*

Remark 2.3.   When the resolvent polynomial $\mathcal{RP}_{\Theta,G,f}(X)$ has a repeated factor, there always exists a suitable Tschirnhausen transformation $\hat{f}$ of f (cf. §3) over M (resp. $X - \hat{\Theta}$ of $X - \Theta$ over k) such that $\mathcal{RP}_{\Theta,G,\hat{f}}(X)$ (resp. $\mathcal{RP}_{\hat{\Theta},G,f}(X)$) has no repeated factors (cf. [Gir83], [Coh93, Alg. 6.3.4], [Col95]).

In the case where $\mathcal{RP}_{\Theta,G,f}(X)$ has no repeated factors, we have the followings:
(i) For $\pi \in G$, the fixed group of the field $M\big(\omega_f(\pi(\Theta))\big)$ corresponds to $\mathrm{Gal}(f) \cap \pi H \pi^{-1}$. In particular, we have $\mathrm{Gal}(\mathcal{RP}_{\Theta,G,f}) \cong \mathrm{Gal}(f)/N$ with $N = \mathrm{Gal}(f) \cap \bigcap_{\pi \in G} \pi H \pi^{-1}$;
(ii) let $\varphi : G \to S_{[G:H]}$ denote the permutation representation of G on the set of left cosets G/H given by the left multiplication. Then we have a realization of the Galois group of $\mathrm{Spl}_M \mathcal{RP}_{\Theta,G,f}(X)$ as a subgroup of the symmetric group $S_{[G:H]}$ by $\varphi(\mathrm{Gal}(f))$.

§3.   Formal Tschirnhausen transformation

We recall the geometric interpretation of a Tschirnhausen transformation which is given in [HM] (see also [HM-3]). Let $f(X)$ be a monic separable polynomial of degree n in $M[X]$ with a fixed order of the roots $\alpha_1, \ldots, \alpha_n$ of $f(X)$ in $\overline{M}$. A Tschirnhausen transformation of $f(X)$ over M is a polynomial of the form

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

Two polynomials $f(X)$ and $g(X)$ in $M[X]$ are Tschirnhausen equivalent over M if they are Tschirnhausen transformations over M of each other. For two irreducible separable

polynomials $f(X)$ and $g(X)$ in $M[X]$, $f(X)$ and $g(X)$ are Tschirnhausen equivalent over M if and only if the quotient fields $M[X]/(f(X))$ and $M[X]/(g(X))$ are M-isomorphic.

In order to obtain an answer to the field intersection problem of k-generic polynomials via multi-resolvent polynomials, we first treat a general polynomial whose roots are n indeterminates $x_1, \ldots, x_n$:

$$f_{\mathbf{s}}(X) = \prod_{i=1}^{n}(X - x_i) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \cdots + (-1)^n s_n \ \in k[\mathbf{s}][X]$$

where $k[x_1, \ldots, x_n]^{S_n} = k[\mathbf{s}] := k[s_1, \ldots, s_n]$, $\mathbf{s} = (s_1, \ldots, s_n)$, and s_i is the i-th elementary symmetric function in n variables $\mathbf{x} = (x_1, \ldots, x_n)$.

Put $R_{\mathbf{x},\mathbf{y}} := k[\mathbf{x}, \mathbf{y}, 1/\Delta_{\mathbf{x}}, 1/\Delta_{\mathbf{y}}]$, where $\mathbf{y} = (y_1, \ldots, y_n)$ consists of n indeterminates, $\Delta_{\mathbf{x}} := \prod_{1 \leq i < j \leq n}(x_j - x_i)$ and $\Delta_{\mathbf{y}} := \prod_{1 \leq i < j \leq n}(y_j - y_i)$. We define the interchanging involution $\iota_{\mathbf{x},\mathbf{y}}$ which exchanges the x_i's and the y_i's:

$$(3.1) \qquad \iota_{\mathbf{x},\mathbf{y}} \ : \ R_{\mathbf{x},\mathbf{y}} \longrightarrow R_{\mathbf{x},\mathbf{y}}, \ x_i \longmapsto y_i, \ y_i \longmapsto x_i, \quad (i = 1, \ldots, n).$$

We take another general polynomial $f_{\mathbf{t}}(X) := \iota_{\mathbf{x},\mathbf{y}}(f_{\mathbf{s}}(X)) \in k[\mathbf{t}][X]$, $\mathbf{t} = (t_1, \ldots, t_n)$, whose roots are n indeterminates $y_1, \ldots, y_n$ where $t_i = \iota_{\mathbf{x},\mathbf{y}}(s_i)$ is the i-th elementary symmetric function in $\mathbf{y} = (y_1, \ldots, y_n)$. We put $K := k(\mathbf{s}, \mathbf{t})$ and $f_{\mathbf{s},\mathbf{t}}(X) := f_{\mathbf{s}}(X) f_{\mathbf{t}}(X)$. The polynomial $f_{\mathbf{s},\mathbf{t}}(X)$ of degree $2n$ is defined over K. We denote

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

Then we have $G_{\mathbf{s},\mathbf{t}} = G_{\mathbf{s}} \times G_{\mathbf{t}}, G_{\mathbf{s}} \cong G_{\mathbf{t}} \cong S_n$ and $k(\mathbf{x}, \mathbf{y})^{G_{\mathbf{s},\mathbf{t}}} = K$.

We intend to apply the results of the previous section for $m = 2n$, $G = G_{\mathbf{s},\mathbf{t}} \leq S_{2n}$ and $f = f_{\mathbf{s},\mathbf{t}}$.

Note that in the splitting field $\mathrm{Spl}_K f_{\mathbf{s},\mathbf{t}}(X) = k(\mathbf{x}, \mathbf{y})$, there exist $n!$ Tschirnhausen transformations from $f_{\mathbf{s}}(X)$ to $f_{\mathbf{t}}(X)$ with respect to $y_{\pi(1)}, \ldots, y_{\pi(n)}$ for $\pi \in S_n$. We shall study the field of definition of each Tschirnhausen transformation from $f_{\mathbf{s}}(X)$ to $f_{\mathbf{t}}(X)$. Let $D := [x_i^{j-1}]_{1 \leq i,j \leq n}$ be the Vandermonde matrix of size n. The matrix $D \in M_n(k(\mathbf{x}))$ is invertible because $\det D = \Delta_{\mathbf{x}}$. The field $k(\mathbf{s})(\Delta_{\mathbf{x}})$ is a quadratic extension of $k(\mathbf{s})$ which corresponds to the fixed field of the alternating group of degree n. We define the n-tuple $(u_0(\mathbf{x}, \mathbf{y}), \ldots, u_{n-1}(\mathbf{x}, \mathbf{y})) \in (R_{\mathbf{x},\mathbf{y}})^n$ by

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

Cramer's rule shows us

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

We write $u_i := u_i(\mathbf{x}, \mathbf{y}), (i = 0, \ldots, n-1)$. The Galois group $G_{\mathbf{s}, \mathbf{t}}$ acts on the orbit $\{\pi(u_i) \mid \pi \in G_{\mathbf{s}, \mathbf{t}}\}$ via regular representation from the left. However this action is not faithful. We put

$$H_{\mathbf{s}, \mathbf{t}} := \{(\pi_{\mathbf{x}}, \pi_{\mathbf{y}}) \in G_{\mathbf{s}, \mathbf{t}} \mid \pi_{\mathbf{x}}(i) = \pi_{\mathbf{y}}(i) \text{ for } i = 1, \ldots, n\} \cong S_n.$$

If $\pi \in H_{\mathbf{s}, \mathbf{t}}$ then we have $\pi(u_i) = u_i$ for $i = 0, \ldots, n-1$. Indeed we see the following:

Lemma 3.1. *For i, $0 \leq i \leq n-1$, u_i is a $G_{\mathbf{s}, \mathbf{t}}$-primitive $H_{\mathbf{s}, \mathbf{t}}$-invariant.*

Let $\Theta := \Theta(\mathbf{x}, \mathbf{y})$ be a $G_{\mathbf{s}, \mathbf{t}}$-primitive $H_{\mathbf{s}, \mathbf{t}}$-invariant. Let $\overline{\pi} = \pi H_{\mathbf{s}, \mathbf{t}}$ be a left coset of $H_{\mathbf{s}, \mathbf{t}}$ in $G_{\mathbf{s}, \mathbf{t}}$. The group $G_{\mathbf{s}, \mathbf{t}}$ acts on the set $\{\pi(\Theta) \mid \overline{\pi} \in G_{\mathbf{s}, \mathbf{t}}/H_{\mathbf{s}, \mathbf{t}}\}$ transitively from the left through the action on the set $G_{\mathbf{s}, \mathbf{t}}/H_{\mathbf{s}, \mathbf{t}}$ of left cosets. Each of the sets $\{\overline{(1, \pi_{\mathbf{y}})} \mid (1, \pi_{\mathbf{y}}) \in G_{\mathbf{s}, \mathbf{t}}\}$ and $\{\overline{(\pi_{\mathbf{x}}, 1)} \mid (\pi_{\mathbf{x}}, 1) \in G_{\mathbf{s}, \mathbf{t}}\}$ forms a complete residue system of $G_{\mathbf{s}, \mathbf{t}}/H_{\mathbf{s}, \mathbf{t}}$, and hence the subgroups $G_{\mathbf{s}}$ and $G_{\mathbf{t}}$ of $G_{\mathbf{s}, \mathbf{t}}$ act on the set $\{\pi(\Theta) \mid \overline{\pi} \in G_{\mathbf{s}, \mathbf{t}}/H_{\mathbf{s}, \mathbf{t}}\}$ transitively. For $\overline{\pi} = \overline{(1, \pi_{\mathbf{y}})} \in G_{\mathbf{s}, \mathbf{t}}/H_{\mathbf{s}, \mathbf{t}}$, we obtain the following equality:

$$y_{\pi_{\mathbf{y}}(i)} = \pi_{\mathbf{y}}(u_0) + \pi_{\mathbf{y}}(u_1)x_i + \cdots + \pi_{\mathbf{y}}(u_{n-1})x_i^{n-1} \text{ for } i = 1, \ldots, n.$$

Hence the set $\{(\pi(u_0), \ldots, \pi(u_{n-1})) \mid \overline{\pi} \in G_{\mathbf{s}, \mathbf{t}}/H_{\mathbf{s}, \mathbf{t}}\}$ gives coefficients of $n!$ different Tschirnhausen transformations from $f_{\mathbf{s}}(X)$ to $f_{\mathbf{t}}(X)$ each of which is defined over $K(\pi(u_0), \ldots, \pi(u_{n-1}))$ respectively.

Definition. We call $K(\pi(u_0), \ldots, \pi(u_{n-1})), (\overline{\pi} \in G_{\mathbf{s}, \mathbf{t}}/H_{\mathbf{s}, \mathbf{t}})$, a field of formal Tschirnhausen coefficients from $f_{\mathbf{s}}(X)$ to $f_{\mathbf{t}}(X)$.

Put $v_i := \iota_{\mathbf{x}, \mathbf{y}}(u_i)$, for $i = 0, \ldots, n-1$. Then v_i is also a $G_{\mathbf{s}, \mathbf{t}}$-primitive $H_{\mathbf{s}, \mathbf{t}}$-invariant, and $K(\pi(v_0), \ldots, \pi(v_{n-1}))$ gives a field of formal Tschirnhausen coefficients from $f_{\mathbf{t}}(X)$ to $f_{\mathbf{s}}(X)$.

Proposition 3.2. *For every $G_{\mathbf{s}, \mathbf{t}}$-primitive $H_{\mathbf{s}, \mathbf{t}}$-invariant Θ, we have $K(\pi(\Theta)) = k(\mathbf{x}, \mathbf{y})^{\pi H_{\mathbf{s}, \mathbf{t}} \pi^{-1}} = K(\pi(u_0), \ldots, \pi(u_{n-1}))$, and $[K(\pi(\Theta)) : K] = n!$ for each $\overline{\pi} \in G_{\mathbf{s}, \mathbf{t}}/H_{\mathbf{s}, \mathbf{t}}$.*

Hence, for each of $n!$ fields $K(\pi(\Theta))$, we have $\mathrm{Spl}_{K(\pi(\Theta))} f_{\mathbf{s}}(X) = \mathrm{Spl}_{K(\pi(\Theta))} f_{\mathbf{t}}(X)$.

Proposition 3.3. *Let Θ be a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant. Then we have*

(i) $K(\mathbf{x}) \cap K(\pi(\Theta)) = K(\mathbf{y}) \cap K(\pi(\Theta)) = K$ *for* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$;

(ii) $K(\mathbf{x},\mathbf{y}) = K(\mathbf{x},\pi(\Theta)) = K(\mathbf{y},\pi(\Theta))$ *for* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$;

(iii) $K(\mathbf{x},\mathbf{y}) = K(\pi(\Theta) \mid \overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}})$.

§4. Field intersection problem

In this section, we explain how to get an answer to the field intersection problem of generic polynomials via multi-resolvent polynomial (cf. [HM], [HM-3]). For $\mathbf{a} = (a_1,\ldots,a_n)$, $\mathbf{b} = (b_1,\ldots,b_n) \in M^n$, we take some fixed order of the roots $\alpha_1,\ldots,\alpha_n$ of $f_{\mathbf{a}}(X)$ and $\beta_1,\ldots,\beta_n$ of $f_{\mathbf{b}}(X)$ in $\overline{M}$, respectively, and denote $L_{\mathbf{a}} := M(\alpha_1,\ldots,\alpha_n)$ and $L_{\mathbf{b}} := M(\beta_1,\ldots,\beta_n)$. We put $f_{\mathbf{a},\mathbf{b}}(X) := f_{\mathbf{a}}(X)f_{\mathbf{b}}(X) \in M[X]$ and define a specialization homomorphism $\omega_{f_{\mathbf{a},\mathbf{b}}}$ by

$$\omega_{f_{\mathbf{a},\mathbf{b}}} : R_{\mathbf{x},\mathbf{y}} \longrightarrow k(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n), \quad \Theta(\mathbf{x},\mathbf{y}) \longmapsto \Theta(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n).$$

Put $\Delta_{\mathbf{a}} := \omega_{f_{\mathbf{a},\mathbf{b}}}(\Delta_{\mathbf{x}})$ and $\Delta_{\mathbf{b}} := \omega_{f_{\mathbf{a},\mathbf{b}}}(\Delta_{\mathbf{y}})$. We assume that both of the polynomials $f_{\mathbf{a}}(X)$ and $f_{\mathbf{b}}(X)$ are separable over M, i.e. $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$. Put $G_{\mathbf{a}} := \mathrm{Gal}(f_{\mathbf{a}}/M)$, $G_{\mathbf{b}} := \mathrm{Gal}(f_{\mathbf{b}}/M)$ and $G_{\mathbf{a},\mathbf{b}} := \mathrm{Gal}(f_{\mathbf{a},\mathbf{b}}/M)$. Then we may naturally regard $G_{\mathbf{a},\mathbf{b}}$ as a subgroup of $G_{\mathbf{s},\mathbf{t}}$. For $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$, we put $c_{j,\pi} := \omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(u_j)), d_{j,\pi} := \omega_{f_{\mathbf{a},\mathbf{b}}}\big(\pi(\iota_{\mathbf{x},\mathbf{y}}(u_j))\big)$, $(j = 0,\ldots,n-1)$. Then for each $i = 1,\ldots,n$, we have

$$\beta_{\pi_{\mathbf{y}}(i)} = c_{0,\pi} + c_{1,\pi}\,\alpha_{\pi_{\mathbf{x}}(i)} + \cdots + c_{n-1,\pi}\,\alpha_{\pi_{\mathbf{x}}(i)}^{n-1},$$

$$\alpha_{\pi_{\mathbf{x}}(i)} = d_{0,\pi} + d_{1,\pi}\,\beta_{\pi_{\mathbf{y}}(i)} + \cdots + d_{n-1,\pi}\,\beta_{\pi_{\mathbf{y}}(i)}^{n-1}.$$

For each $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$, there exists a Tschirnhausen transformation from $f_{\mathbf{a}}(X)$ to $f_{\mathbf{b}}(X)$ over the field of Tschirnhausen coefficients $M(c_{0,\pi},\ldots,c_{n-1,\pi})$. From the assumption $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, we first see the following lemma (cf. [JLY02, p. 141], [HM]).

Lemma 4.1. *Let M'/M be a field extension. If $f_{\mathbf{b}}(X)$ is a Tschirnhausen transformation of $f_{\mathbf{a}}(X)$ over M', then $f_{\mathbf{a}}(X)$ is a Tschirnhausen transformation of $f_{\mathbf{b}}(X)$ over M'. In particular, we have $M(c_{0,\pi},\ldots,c_{n-1,\pi}) = M(d_{0,\pi},\ldots,d_{n-1,\pi})$ for every $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$.*

To obtain an answer to the field intersection problem of $f_{\mathbf{s}}(X)$ we study the $n!$ fields $M(c_{0,\pi},\ldots,c_{n-1,\pi})$ of Tschirnhausen coefficients from $f_{\mathbf{a}}(X)$ to $f_{\mathbf{b}}(X)$ over M.

Proposition 4.2. *Under the assumption $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, we have*

(i) $\mathrm{Spl}_{M(c_{0,\pi},\ldots,c_{n-1,\pi})} f_{\mathbf{a}}(X) = \mathrm{Spl}_{M(c_{0,\pi},\ldots,c_{n-1,\pi})} f_{\mathbf{b}}(X)$ *for each* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$;

(ii) $L_{\mathbf{a}}L_{\mathbf{b}} = L_{\mathbf{a}}\,M(c_{0,\pi},\ldots,c_{n-1,\pi}) = L_{\mathbf{b}}\,M(c_{0,\pi},\ldots,c_{n-1,\pi})$ *for each* $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$.

Applying the specialization $\omega_{f_{\mathbf{a},\mathbf{b}}}$, we take the $G_{\mathbf{s},\mathbf{t}}$-relative $H_{\mathbf{s},\mathbf{t}}$-invariant resolvent polynomial of $f_{\mathbf{a},\mathbf{b}}$ by a $G_{\mathbf{s},\mathbf{t}}$-primitive $H_{\mathbf{s},\mathbf{t}}$-invariant Θ:

$$\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}}(X) = \prod_{\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}} \big(X - \omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(\Theta))\big) \in M[X].$$

The resolvent polynomial $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}}(X)$ is also called an (absolute) multi-resolvent (cf. [GLV88], [RV99], [Val]).

Proposition 4.3.   *For $\mathbf{a},\mathbf{b} \in M^n$ with $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, suppose that the polynomial $\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}}(X)$ has no repeated factors. Then the following two assertions hold:*
(i) $M(c_{0,\pi}, \ldots, c_{n-1,\pi}) = M\big(\omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(\Theta))\big)$ *for each $\overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$;*
(ii) $\mathrm{Spl}_M f_{\mathbf{a},\mathbf{b}}(X) = M(\omega_{f_{\mathbf{a},\mathbf{b}}}(\pi(\Theta)) \mid \overline{\pi} \in G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}).$

Definition.   For a separable polynomial $f(X) \in M[X]$ of degree d, the decomposition type of $f(X)$ over M, denoted by $\mathrm{DT}(f/M)$, is defined as the partition of d induced by the degrees of the irreducible factors of $f(X)$ over M. We define the decomposition type $\mathrm{DT}(\mathcal{RP}_{\Theta,G,f}/M)$ of $\mathcal{RP}_{\Theta,G,f}(X)$ over M by $\mathrm{DT}(\mathcal{RP}_{\Theta,G,\hat{f}}/M)$ where $\hat{f}(X)$ is a Tschirnhausen transformation of $f(X)$ over M which satisfies that $\mathcal{RP}_{\Theta,G,\hat{f}}(X)$ has no repeated factors (cf. Remark 2.3).

We write $\mathrm{DT}(f) := \mathrm{DT}(f/M)$ for simplicity. From Theorem 2.1, the decomposition type $\mathrm{DT}(\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}})$ coincides with the partition of $n!$ induced by the lengths of the orbits of $G_{\mathbf{s},\mathbf{t}}/H_{\mathbf{s},\mathbf{t}}$ under the action of $\mathrm{Gal}(f_{\mathbf{a},\mathbf{b}})$. Hence, by Proposition 4.3, $\mathrm{DT}(\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}})$ gives the degrees of $n!$ fields of Tschirnhausen coefficients from $f_{\mathbf{a}}(X)$ to $f_{\mathbf{b}}(X)$ over M.

We conclude that $\mathrm{DT}(\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}})$ gives us information about the field intersection problem for $f_{\mathbf{s}}(X)$ through the degrees of the fields of Tschirnhausen coefficients $M(c_{0,\pi}, \ldots, c_{n-1,\pi})$ over M and is determined by the degeneration of the Galois group $\mathrm{Gal}(f_{\mathbf{a},\mathbf{b}})$ under the specialization $(\mathbf{s}, \mathbf{t}) \mapsto (\mathbf{a}, \mathbf{b})$. As a special case of the field intersection problem, we get the followings:

Theorem 4.4 ([HM-3]).   *For $\mathbf{a},\mathbf{b} \in M^n$ with $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, the quotient fields $M[X]/(f_{\mathbf{a}}(X))$ and $M[X]/(f_{\mathbf{b}}(X))$ are M-isomorphic if and only if the decomposition type $\mathrm{DT}(\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}})$ over M includes 1.*

Corollary 4.5 (The field isomorphism problem).   *For $\mathbf{a},\mathbf{b} \in M^n$ with $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$, we assume that both of $G_{\mathbf{a}}$ and $G_{\mathbf{b}}$ are isomorphic to a transitive subgroup $G \leq S_n$ and that all subgroups of G with index n are conjugate in G. Then $\mathrm{DT}(\mathcal{RP}_{\Theta,G_{\mathbf{s},\mathbf{t}},f_{\mathbf{a},\mathbf{b}}})$ over M includes 1 if and only if $\mathrm{Spl}_M f_{\mathbf{a}}(X)$ and $\mathrm{Spl}_M f_{\mathbf{b}}(X)$ coincide.*

§5.   Field intersection problem: the case of S_3

We take $f_s^{S_3}(X) = X^3 + sX + s \in k(s)[X]$. For $a, b \in M$, we put $L_a := \mathrm{Spl}_M f_a^{S_3}(X)$ and $G_a := \mathrm{Gal}(f_a^{S_3}/M), G_{a,b} := \mathrm{Gal}(f_a^{S_3} f_b^{S_3}/M)$. For $a, b \in M$, we assume that $ab(4a + 27)(4b + 27) \neq 0$ because the discriminant of $f_s^{S_3}(X)$ equals $-s^2(4s + 27)$.

In the case of char $k \neq 3$, we take a $G_{\mathbf{s,t}}$-primitive $H_{\mathbf{s,t}}$-invariant $\Theta := 3u_1/u_2$ where u_1 and u_2 are formal Tschirnhausen coefficients which are given in Section 3. Then we may evaluate

$$F_{s,t}(X) := (s - t) \cdot \mathcal{RP}_{\Theta, G_{\mathbf{s,t}}, f_s^{S_3} f_t^{S_3}}(X) = (s - t) \cdot \prod_{\overline{\pi} \in G_{\mathbf{s,t}}/H_{\mathbf{s,t}}} (X - \pi(\Theta)) \in k(s, t)[X]$$

$$= s(X^2 + 9X - 3s)^3 - t(X^3 - 2sX^2 - 9sX - 2s^2 - 27s)^2.$$

The discriminant of $F_{s,t}(X)$ is $s^{10}t^4(4s + 27)^{15}(4t + 27)^3$. Note that, for $a, b \in M$ with $ab(4a + 27)(4b + 27) \neq 0$, $F_{a,b}(X)$ has no repeated factors. In the case of char $k = 3$, we may take $\Theta = u_0$, the constant term of a formal Tschirnhausen transformation, as a suitable $G_{\mathbf{s,t}}$-primitive $H_{\mathbf{s,t}}$-invariant. Then we get squarefree $\mathcal{RP}_{u_0, G_{\mathbf{s,t}}, f_s^{S_3} f_t^{S_3}}(X)$ as we mentioned in Remark 2.3 (see [HM]).

Theorem 5.1 ([HM]).   *Assume that char $k \neq 3$. For $a, b \in M$, we also assume that $a \neq b$ and $\#G_a \geq \#G_b > 1$. Then an answer to the field intersection problem for $f_s^{S_3}(X)$ is given by* $\mathrm{DT}(F_{a,b})$ *as Table 1 shows.*

Table 1

G_a	G_b	$G_{a,b}$		$\mathrm{DT}(F_{a,b})$
S_3	S_3	$S_3 \times S_3$	$L_a \cap L_b = M$	6
		$(C_3 \times C_3) \rtimes C_2$	$[L_a \cap L_b : M] = 2$	$3, 3$
		S_3	$L_a = L_b$	$3, 2, 1$
	C_3	$S_3 \times C_3$	$L_a \cap L_b = M$	6
	C_2	D_6	$L_a \not\supset L_b$	6
		S_3	$L_a \supset L_b$	$3, 3$
C_3	C_3	$C_3 \times C_3$	$L_a \neq L_b$	$3, 3$
		C_3	$L_a = L_b$	$3, 1, 1, 1$
	C_2	C_6	$L_a \cap L_b = M$	6
C_2	C_2	$C_2 \times C_2$	$L_a \neq L_b$	$4, 2$
		C_2	$L_a = L_b$	$2, 2, 1, 1$

As a special case of Theorem 5.1 (cf. Theorem 4.4 and Corollary 4.5), we get Theorem 1.2 which we introduced in Section 1.

Proof of Theorem 1.2. Because the polynomial $F_{s,t}(X) = s(X^2 + 9X - 3s)^3 - t(X^3 - 2sX^2 - 9sX - 2s^2 - 27s)^2$ is linear in t, we see that $F_{a,b}(X)$ has a root in M if and only if there exists $u \in M$ such that

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

§ 6. Field intersection problem: the case of D_5

Let $\sigma := (12345)$, $\rho := (1243)$, $\tau := \rho^2$, $\omega := (12) \in S_5$ act on $k(x_1, \ldots, x_5)$ by $\pi(x_i) = x_{\pi(i)}, (\pi \in S_5)$. For simplicity, we write

$$C_5 = \langle \sigma \rangle, \quad D_5 = \langle \sigma, \tau \rangle, \quad F_{20} = \langle \sigma, \rho \rangle, \quad S_5 = \langle \sigma, \omega \rangle.$$

We take the cross-ratios

$$x := \xi(x_1, \ldots, x_5) = \frac{x_1 - x_4}{x_1 - x_3} \bigg/ \frac{x_2 - x_4}{x_2 - x_3}, \quad y := \eta(x_1, \ldots, x_5) = \frac{x_2 - x_5}{x_2 - x_4} \bigg/ \frac{x_3 - x_5}{x_3 - x_4}.$$

Then S_5 acts faithfully on $k(x, y)$ as

$$\sigma \ : \ x \longmapsto y, \ y \longmapsto -(y-1)/x, \quad \rho \ : \ x \longmapsto x/(x-1), \ y \longmapsto (y-1)/(x+y-1),$$

$$\tau \ : \ x \longmapsto x, \ y \longmapsto -(x-1)/y, \quad \omega \ : \ x \longmapsto 1/x, \ y \longmapsto (x+y-1)/x.$$

We take a k-generic polynomial $f_{s,t}^{D_5}(X) \in k(s,t)[X]$ as the formal D_5-relative $\langle \tau \rangle$-invariant resolvent polynomial by x:

$$f_{s,t}^{D_5}(X) := \mathcal{RP}_{x,D_5}(X) = \left(X - x \right)\left(X - y \right)\left(X - \frac{1-y}{x} \right)\left(X - \frac{x+y-1}{xy} \right)\left(X - \frac{1-x}{y} \right)$$

$$= X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2-t-2s-1)X^2 + sX + t.$$

Note that $k(s,t) = k(x,y)^{D_5}$. We take two fields $k(\mathbf{x}) = k(x,y)$ and $k(\mathbf{x}') = k(x',y')$ where $x' := \xi(y_1, \ldots, y_5)$, $y' := \eta(y_1, \ldots, y_5)$ and the interchanging involution

$$\iota \ : \ k(\mathbf{x}, \mathbf{x}') \longrightarrow k(\mathbf{x}, \mathbf{x}'), \quad (x, y, x', y') \longmapsto (x', y', x, y)$$

which is induced by the $\iota_{\mathbf{x},\mathbf{y}}$ of (3.1). We put $(s', t', d') := \iota(s, t, d)$, $\mathbf{s}' := (s', t')$ and $(\sigma', \tau', \rho') := (\iota^{-1}\sigma\iota, \iota^{-1}\tau\iota, \iota^{-1}\rho\iota) \in \mathrm{Aut}_k(k(x', y'))$ and write

$$D_5' = \langle \sigma', \tau' \rangle, \quad F_{20}' = \langle \sigma', \rho' \rangle \quad \text{and} \quad D_5'' = \langle \sigma\sigma', \tau\tau' \rangle.$$

We now take the $D_5 \times D_5'$-primitive D_5''-invariant

$$P := xx' + yy' + \frac{(y-1)(y'-1)}{xx'} + \frac{(x+y-1)(x'+y'-1)}{xx'yy'} + \frac{(x-1)(x'-1)}{yy'}$$

and the formal $D_5 \times D_5'$-relative D_5''-invariant resolvent polynomial by P:

$$(6.1) \qquad F_{\mathbf{s},\mathbf{s}'}^1(X) := \mathcal{RP}_{P, D_5 \times D_5'}(X) = \prod_{\overline{\pi} \in (D_5 \times D_5')/D_5''} (X - \pi(P))$$

$$= \left(X^5 - (t-3)(t'-3)X^4 + c_3 X^3 + \frac{c_2}{2} X^2 + \frac{c_1}{2} X + \frac{c_0}{2} \right)^2$$

$$- \frac{d^2 d'^2}{4}\left(X^2 + (t+t'-1)X + (s-t+s'-t'+tt'+2) \right)^2 ;$$

here $c_3, c_2, c_1, c_0 \in k(s,t,s',t')$ are given by

$c_3 = \left[2s - 21t + 3t^2 - 2ts' + t^2s' - t^2t' \right] + 31 - 3ss' + 5tt',$

$c_2 = \left[-20s + 112t + 8st - 32t^2 + 2t^3 + 5ts' - 13sts' - 12t^2s' + 4t^3s' - 15stt' \right.$

$\qquad \left. + 14t^2t' + 2t^3t' + 8t^2s't' - 2t^3t'^2 \right] - 102 + 27ss' - 119tt' - sts't' + 6t^2t'^2,$

$c_1 = \left[32s + 2s^2 - 128t - 26st + 60t^2 + 4st^2 - 8t^3 - 6s^2s' - 7ts' + 38sts' + 9t^2s' - 5st^2s' \right.$

$\qquad - 12t^3s' + 2t^4s' - 20ts'^2 - 8sts'^2 + 6t^2s'^2 + 2t^3s'^2 + 2stt' - 77t^2t' + 3st^2t' + 8t^3t' - 29t^2s't'$

$\qquad \left. + st^2s't' + 18t^3s't' - 2st^2t'^2 + 10t^3t'^2 \right] + 80 - 37ss' + 145tt' - 45sts't' + 24t^2t'^2 - 8t^3t'^3,$

$c_0 = \left[-16s - 2s^2 + 56t + 24st + 2s^2t - 38t^2 - 8st^2 + 8t^3 + 5s^2s' - 2ts' - 38sts' - 7s^2ts' \right.$

$\qquad + 5t^2s' + 13st^2s' + 8t^3s' + 2st^3s' - 4t^4s' - 21ts'^2 - 11sts'^2 - 2t^2s'^2 + 2st^2s'^2 + 4t^3s'^2$

$\qquad - 104stt' - 33s^2tt' + 105t^2t' + 35st^2t' + 4t^3t' + 16st^3t' - 6t^4t' - 2t^5t' - s^2ts't' + 36t^2s't'$

$\qquad - 14st^2s't' - 6t^3s't' + 6t^4s't' + 8t^2s'^2t' - 37st^2t'^2 + 22t^3t'^2 - 2st^3t'^2 + 8t^4t'^2 + 8t^3s't'^2$

$\qquad \left. - 2t^4t'^3 \right] - 24 + 14ss' - 8s^2s'^2 - 224tt' + sts't' - 101t^2t'^2 - st^2s't'^2 - 8t^3t'^3$

where $\left[a \right] := a + \iota(a)$ for $a \in k(s,t,s',t')$, and $d^2 \in k(s,t)$ is given by the formula

$$d^2 = s^2 - 4s^3 + 4t - 14st - 30s^2t - 91t^2 - 34st^2 + s^2t^2 + 40t^3 + 24st^3 + 4t^4 - 4t^5.$$

We also take $\rho(P) \in k(s,t)$ which is conjugate of P under the action of $F_{20} \times F'_{20}$ but not so under the action of $D_5 \times D'_5$. Put

$$F^2_{\mathbf{s},\mathbf{s}'}(X) := \mathcal{RP}_{\rho(P), D_5 \times D'_5}(X) = F^1_{\rho(s),\rho(t),s',t'}(X) = \rho\big(F^1_{\mathbf{s},\mathbf{s}'}(X)\big).$$

For $\mathbf{a} = (a_1, a_2) \in M^2$, we denote $L_{\mathbf{a}} := \mathrm{Spl}_M f^{D_5}_{\mathbf{a}}(X)$, $G_{\mathbf{a}} := \mathrm{Gal}(f^{D_5}_{\mathbf{a}})$ and $G_{\mathbf{a},\mathbf{a}'} := \mathrm{Gal}(f^{D_5}_{\mathbf{a}} f^{D_5}_{\mathbf{a}'})$. We now state the result of the dihedral quintic case.

Theorem 6.1 ([HM-3]).   *For* $\mathbf{a} = (a_1, a_2)$, $\mathbf{a}' = (a'_1, a'_2) \in M^2$, *we assume* $\#G_{\mathbf{a}} \geq \#G_{\mathbf{a}'} > 1$. *An answer to the field intersection problem for* $f^{D_5}_{s,t}(X)$ *is given by the decomposition types* $\mathrm{DT}(F^1_{\mathbf{a},\mathbf{a}'})$ *and* $\mathrm{DT}(F^2_{\mathbf{a},\mathbf{a}'})$ *over* M *as Table 2 shows.*

Table 2

$G_{\mathbf{a}}$	$G_{\mathbf{a}'}$	$G_{\mathbf{a},\mathbf{a}'}$		$\mathrm{DT}(F^1_{\mathbf{a},\mathbf{a}'})$	$\mathrm{DT}(F^2_{\mathbf{a},\mathbf{a}'})$
D_5	D_5	$D_5 \times D_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
		$(C_5 \times C_5) \rtimes C_2$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 2$	$5,5$	$5,5$
		D_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5,2,2,1$	$5,5$
				$5,5$	$5,2,2,1$
	C_5	$D_5 \times C_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
	C_2	D_{10}	$L_{\mathbf{a}} \not\supset L_{\mathbf{a}'}$	10	10
		D_5	$L_{\mathbf{a}} \supset L_{\mathbf{a}'}$	$5,5$	$5,5$
C_5	C_5	$C_5 \times C_5$	$L_{\mathbf{a}} \neq L_{\mathbf{a}'}$	$5,5$	$5,5$
		C_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5,1,1,1,1,1$	$5,5$
				$5,5$	$5,1,1,1,1,1$
	C_2	C_{10}	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
C_2	C_2	$C_2 \times C_2$	$L_{\mathbf{a}} \neq L_{\mathbf{a}'}$	$4,4,2$	$4,4,2$
		C_2	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$2,2,2,2,1,1$	$2,2,2,2,1,1$

We checked the decomposition types on Table 2 using the computer algebra system GAP [GAP].

Remark 6.2. In the cases of $G_{\mathbf{a}} = D_5$, C_2, the quadratic subextension of L_{s_1,t_1} over M for $(s_1, t_1) \in M^2$ is given by

$$M\left(\sqrt{s_1^2 - 4s_1^3 + 4t_1 - 14s_1t_1 - 30s_1^2t_1 - 91t_1^2 - 34s_1t_1^2 + s_1^2t_1^2 + 40t_1^3 + 24s_1t_1^3 + 4t_1^4 - 4t_1^5}\right).$$

Remark 6.3. As is well known, for a suitable integer l, we may have an answer to the field intersection problem via the formal $D_5 \times D_5'$-relative $\langle \tau \rangle \times \langle \tau' \rangle$-invariant resolvent polynomial $G_{\mathbf{s},\mathbf{s}'}(X) := \mathcal{RP}_{x+lx', D_5 \times D_5'}(X)$ by $x + lx'$ (cf. [Coh93], [Coh00]). Although the degree of the multi-resolvent polynomials $F_{\mathbf{s},\mathbf{s}'}^1(X)$ and $F_{\mathbf{s},\mathbf{s}'}^1(X)$ with respect to X is 10, the degree of $G_{\mathbf{s},\mathbf{s}'}(X)$ is 25 and an explicit formula of $G_{\mathbf{s},\mathbf{s}'}(X)$ in terms of $\mathbf{s}$ and $\mathbf{s}'$ is very complicated. We remark that to construct a suitable explicit formula is significant to investigate the structure of all G-Galois extensions over M (cf. Section 1 and Corollaries 1.4 and 1.5).

Example 6.4. Take $M = \mathbb{Q}$, $\mathbf{a} = (0, 3)$ and $\mathbf{a}' = (10, 3)$. Then we have

$$F_{\mathbf{a},\mathbf{a}'}^1(X) = (X + 5)^3(X^2 - 15X + 150)(X^5 - 625X^2 - 9375),$$

$$F_{\mathbf{a},\mathbf{a}'}^2(X) = \left(X^5 - \frac{125}{9}X^3 + \frac{6250}{81}X - \frac{3125}{27}\right)\left(X^5 - \frac{125}{9}X^3 + \frac{625}{9}X^2 + \frac{15625}{81}X + \frac{15625}{27}\right).$$

The decomposition type of $F_{\mathbf{a},\mathbf{a}'}^1(X)$ over $\mathbb{Q}$ should be $5, 2, 2, 1$ (cf. also Theorem 2.1); and hence we conclude that $\mathrm{Spl}_{\mathbb{Q}} f_{\mathbf{a}}^{D_5}(X) = \mathrm{Spl}_{\mathbb{Q}} f_{\mathbf{a}'}^{D_5}(X)$ and $G_{\mathbf{a}} = D_5$.

From the viewpoint of Diophantine geometry, we give some numerical examples of the field isomorphism problem of $f_{s,t}^{D_5}(X)$ over $M = \mathbb{Q}$ and for integral points $\mathbf{a}, \mathbf{a}' \in \mathbb{Z}^2$ using Theorem 6.1 and the explicit formula (6.1). We do not know, however, for a given $\mathbf{a} \in \mathbb{Z}^2$ whether there exist only finitely many $\mathbf{a}' \in \mathbb{Z}^2$ such that $\mathrm{Spl}_{\mathbb{Q}} f_{\mathbf{a}}^{D_5}(X) = \mathrm{Spl}_{\mathbb{Q}} f_{\mathbf{a}'}^{D_5}(X)$ or not (cf. Corollary 1.5).

Example 6.5. Take $M = \mathbb{Q}$ and $t := 1$. Then we have $f_{s,1}^{D_5}(X) = X^5 - 2X^4 + (s+2)X^3 - (2s+1)X^2 + sX + 1$. For $s_1, s_1' \in \mathbb{Z}$ in the range $-10000 \leq s_1 < s_1' \leq 10000$, $\mathrm{Spl}_{\mathbb{Q}} f_{s_1,1}^{D_5}(X) = \mathrm{Spl}_{\mathbb{Q}} f_{s_1',1}^{D_5}(X)$ if and only if $(s_1, s_1') \in X_1 \cup X_2$ where

$$X_1 = \{(-6, 0), (-1, 41), (-94, -10)\},$$
$$X_2 = \{(-1, 0), (-6, -1), (-18, -7), (1, 34), (0, 41), (-6, 41), (-167, -8)\}.$$

It was directly checked by Theorem 6.1 that, in the range $-10000 \leq s_1 < s_1' \leq 10000$, $(s_1, s_1') \in X_i$ if and only if $\mathrm{DT}(F_{s_1,1,s_1',1}^i/\mathbb{Q})$ includes 1, for each of $i = 1, 2$.

Example 6.6. Kida-Renault-Yokoyama [KRY] showed that there exist infinitely many $b \in \mathbb{Q}$ such that $\mathrm{Spl}_{\mathbb{Q}} f_{0,1}^{D_5}(X) = \mathrm{Spl}_{\mathbb{Q}} f_{b,1}^{D_5}(X)$. Their method enables us to construct such b's explicitly via rational points of an associated elliptic curve (cf. [KRY]).

They also pointed out that in the range $-400 \leq s_1, t_1 \leq 400$ there are 25 pairs $(s_1, t_1) \in \mathbb{Z}^2$ such that $\mathrm{Spl}_{\mathbb{Q}} f_{0,1}^{D_5}(X) = \mathrm{Spl}_{\mathbb{Q}} f_{s_1,t_1}^{D_5}(X)$. We may classify the 25 pairs by the polynomials $F_{0,1,s_1,t_1}^1(X)$ and $F_{0,1,s_1,t_1}^2(X)$. In the range above, for $i = 1, 2$, $\mathrm{DT}(F_{0,1,s_1,t_1}^i/\mathbb{Q})$ includes 1 if and only if $(s_1, t_1) \in X_i$ where

$$X_1 = \{(0,1), (4,-1), (4,5), (-6,1), (-24,19), (34,11), (36,-5),$$
$$(46,-1), (-188,23), (264,31), (372,-5), (378,43)\},$$
$$X_2 = \{(-1,-1), (-1,1), (5,-1), (41,1), (-43,5), (47,13), (59,-5),$$
$$(59,19), (101,19), (125,-23), (149,11), (155,25), (-169,55)\}.$$

By Theorem 6.1, we checked such pairs in the range $-20000 \leq s_1, t_1 \leq 20000$; and added six pairs $(526,41), (952,113), (2302,95), (6466,311), (7180,143)$ and $(7480,-169)$ to X_1 and just four pairs $(785,-25), (3881,29), (-11215,299)$ and $(19739,-281)$ to X_2.

Example 6.7.   Take the k-generic polynomial $g_{A,B}^{C_5}(X) \in k(A,B)[X]$ for C_5 which is constructed by Hashimoto-Tsunogai [HT03]:

$$g_{A,B}^{C_5}(X) = X^5 - \frac{P}{Q^2}(A^2 - 2A + 15B^2 + 2)X^3 + \frac{P^2}{Q^3}(2BX^2 - (A-1)X - 2B)$$

where $P = (A^2 - A - 1)^2 + 25(A^2 + 1)B^2 + 125B^4$, $Q = (A+7)B^2 - A + 1$. We may apply Theorem 6.1 to $g_{A,B}^{C_5}(X)$ since there exist $s_1, t_1 \in k(A,B)$ such that $\mathrm{Spl}_{k(A,B)} f_{s_1,t_1}^{D_5}(X) = \mathrm{Spl}_{k(A,B)} g_{A,B}^{C_5}(X)$ (cf. [HT03], [HM-3]). For $\mathbf{a} = (a, b)$, $\mathbf{a}' = (a', b') \in \mathbb{Z}^2$, if $\mathbf{a}' = (a, \pm b)$ or $\{\mathbf{a}, \mathbf{a}'\} = \{(-1, \pm b), (1, \pm b)\}$ then $\mathrm{Spl}_{\mathbb{Q}} g_{a,b}^{C_5}(X) = \mathrm{Spl}_{\mathbb{Q}} g_{a',b'}^{C_5}(X)$ (cf. [HM-3]). For $\mathbf{a}, \mathbf{a}' \in \mathbb{Z}^2$ in the range $-50 \leq a, a' \leq 50$, $0 \leq b \leq b' \leq 50$ with $\mathbf{a} \neq \mathbf{a}'$, $\{\mathbf{a}, \mathbf{a}'\} \neq \{(-1, b), (1, b)\}$, we see that $\mathrm{Spl}_{\mathbb{Q}} g_{a,b}^{C_5}(X) = \mathrm{Spl}_{\mathbb{Q}} g_{a',b'}^{C_5}(X)$ if and only if $(a, b, a', b') \in X_1 \cup X_2$ where

$$X_1 = \{(-3,1,-3,11), (3,3,23,3), (23,3,3,3), (7,3,27,9),$$
$$(2,2,-28,14), (8,11,33,14), (23,5,35,7), (41,11,-15,17)\},$$
$$X_2 = \{(-2,1,3,2), (4,1,-6,2), (3,1,13,7), (16,2,-12,5), (-2,2,18,4), (31,1,-19,7),$$
$$(-3,3,-33,3), (-33,3,-3,3), (-16,13,34,19), (-2,3,43,6), (12,4,46,10)\}.$$

By Theorem 6.1, it can be checked, in the range above and for each of $i = 1, 2$, that $(a, b, a', b') \in X_i$ if and only if the decomposition type of $F_{\mathbf{a},\mathbf{a}'}^i(X)$ over $\mathbb{Q}$ includes 1.

Example 6.8.   Let $h_n(X)$ be Lehmer's simplest quintic polynomial

$$h_n(X) = X^5 + n^2 X^4 - (2n^3 + 6n^2 + 10n + 10)X^3$$
$$+ (n^4 + 5n^3 + 11n^2 + 15n + 5)X^2 + (n^3 + 4n^2 + 10n + 10)X + 1$$

(cf. [Leh88]), and take $M = \mathbb{Q}$. We regard n as an independent parameter over $\mathbb{Q}$. By the result in [HR], for Brumer's quintic $f_{s,t}^{D_5}(X)$, we see that $\mathrm{Spl}_{\mathbb{Q}(n)} h_n(X) =$

$\mathrm{Spl}_{\mathbb{Q}(n)} f_{s,t}^{D_5}(X)$ where $s = -20 - 5n + 10n^2 + 12n^3 + 5n^4 + n^5$, $t = -7 - 10n - 5n^2 - n^3$. By Theorem 6.1, we checked pairs $(n, n') \in \mathbb{Z}^2$ in the range $-10000 \leq n < n' \leq 10000$ to confirm that $\mathrm{Spl}_{\mathbb{Q}} h_n(X) = \mathrm{Spl}_{\mathbb{Q}} h_{n'}(X)$ if and only if $(n, n') = (-2, -1)$.

References

[Ade01] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, 1761, Springer, 2001.

[AV00] P. Aubry, A. Valibouze, *Using Galois ideals for computing relative resolvents*, Algorithmic methods in Galois theory. J. Symbolic Comput. **30** (2000), 635–651.

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

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

[Coh00] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, 193, Springer, 2000.

[Col95] A. Colin, *Formal computation of Galois groups with relative resolvents*, 169–182, Lecture Notes in Comput. Sci., 948, Springer, 1995.

[DeM83] F. R. DeMeyer, *Generic Polynomials*, J. Algebra **84** (1983), 441–448.

[GAP] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.10; 2007 (http://www.gap-system.org).

[GK00] K. Geissler, J. Klüners, *Galois group computation for rational polynomials*, Algorithmic methods in Galois theory. J. Symbolic Comput. **30** (2000), 653–674.

[Gir83] K. Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math. **43** (1983), 289–307.

[GLV88] M. Giusti, D. Lazard, A. Valibouze, *Algebraic transformations of polynomial equations, symmetric polynomials and elimination*, Symbolic and algebraic computation (Rome, 1988), 309–314, Lecture Notes in Comput. Sci., 358, Springer, 1989.

[Has00] K. Hashimoto, *On Brumer's family of RM-curves of genus two*, Tohoku Math. J. **52** (2000), 475–488.

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

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

[HT03] K. Hashimoto and H. Tsunogai, *Generic Polynomials over* **Q** *with two parameters for the transitive groups of degree five*, Proc. Japan. Acad. Ser. A **79** (2003), 142–145.

[HM07] A. Hoshi, K. Miyake, *Tschirnhausen transformation of a cubic generic polynomial and a 2-dimensional involutive Cremona transformation*, Proc. Japan Acad. Ser. 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]

[HM-2]   A. Hoshi, K. Miyake, *On the field intersection problem of quartic generic polynomials via formal Tschirnhausen transformation*, preprint. arXiv:0812.4807v1 [math.NT]

[HM-3]   A. Hoshi, K. Miyake, *On the field intersection problem of solvable quintic generic polynomials*, preprint. arXiv:0804.4875v1 [math.NT]

[HR]   A. Hoshi, Y. Rikuna, *On a transformation from dihedral quintic polynomials into Brumer's form*, in preparation.

[JLY02]   C. Jensen, A. Ledet, N. Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, 45, Cambridge, 2002.

[Kem94]   G. Kemper, *Das Noethersche Problem und generische Polynome*, Dissertation, University of Heidelberg, 1994, also available as: IWR Preprint 94-49, Heidelberg.

[KM00]   G. Kemper, E. Mattig, *Generic polynomials with few parameters*, Algorithmic methods in Galois theory. J. Symbolic Comput. **30** (2000), 843–857.

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

[Kid05]   M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), 427–447.

[Kid06]   M. Kida, *Cyclic polynomials arising from Kummer theory of norm algebraic tori*, Algorithmic number theory, 102–113, Lecture Notes in Comput. Sci., 4076, Springer, 2006.

[KRY]   M. Kida, G. Renault, K. Yokoyama, *Quintic polynomials of Hashimoto-Tsunogai, Brumer, and Kummer*, to appear in Int. J. Number Theory.

[Kom]   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`

[Lag1770] J. Lagrange, *Réflexions sur la résolution algébrique des équations*, Mémoires de l'Académie de Berlin (1770), 205–421.

[Lan78]   S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften 231, Springer, 1978.

[Leh88]   E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535–541.

[MM97]   T. Mattman, J. McKay, *Computation of Galois groups over function fields*, Math. Comp. **66** (1997), 823–831.

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

[RV99]   N. Rennert, A. Valibouze, *Calcul de résolvantes avec les modules de Cauchy*, Experiment. Math. **8** (1999), 351–366.

[Rik04]   Y. Rikuna, *Explicit constructions of generic polynomials for some elementary groups*, Galois theory and modular forms, 173–194, Dev. Math., 11, Kluwer Acad. Publ., Boston, MA, 2004.

[SM85]   L. Soicher, J. McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), 273–281.

[Sta73]   R. P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

[Val95]   A. Valibouze, *Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems*, 456–468, Lecture Notes in Comput. Sci., 948, Springer, 1995.

[Val]   A. Valibouze, *Galois theory and reducible polynomials*. Available from `http://www.lix.polytechnique.fr/~max/publications/valibouze/jnt99.dvi`

[Wol03] S. Wolfram, *The Mathematica Book, Fifth Edition*, Wolfram Media, Inc., Cambridge University Press, 2003.

[Yok97] K. Yokoyama, *A modular method for computing the Galois groups of polynomials*, J. Pure Appl. Algebra 117/118 (1997), 617–636.