Generic sextic polynomial related to the subfield problem of a cubic polynomial

Komatsu, Toru
Faculty of Mathematics, Kyushu University

https://hdl.handle.net/2324/3383

出版情報：MHF Preprint Series. 2006-9, 2006-03-09. 九州大学大学院数理学研究院
バージョン：

MHF Preprint Series

Kyushu University
21st Century COE Program
Development of Dynamic Mathematics with High Functionality

Generic sextic polynomial related to the subfield problem of a cubic polynomial

T. Komatsu

MHF 2006-9

(Received March 9, 2006)

Faculty of Mathematics
Kyushu University
Fukuoka, JAPAN

Generic sextic polynomial related to the subfield problem of a cubic polynomial

Toru KOMATSU

§ 1. Introduction

In this paper we solve the subfield problem of a generic cubic polynomial $g(t, Y)$ for the symmetric group $\mathfrak{S}_3$ of degree 3 by using a certain sextic polynomial $P(\mathfrak{t}, Z)$ which is generic for the direct product $(\mathfrak{S}_3)^2$ of the two groups $\mathfrak{S}_3$. We also study the descent genericity of the polynomial $P(\mathfrak{t}, Z)$ explicitly. See § 2 for the notion about the genericity of a polynomial and the subfield problem of the polynomial.

Let k be a field with $\mathrm{char}(k) \neq 2, 3$ and $k(t)$ the rational function field over k in one variable t. Let $g(t, Y)$ be a cubic polynomial over $k(t)$ of the form

$$g(t, Y) = Y^3 - tY - t = Y^3 - t(Y + 1).$$

Let $k(\mathfrak{t})$ be the rational function field over k with two variables t_1 and t_2 where $\mathfrak{t} = (t_1, t_2)$. We define a sextic polynomial $P(\mathfrak{t}, Z) \in k(\mathfrak{t})[Z]$ over $k(\mathfrak{t})$ by

$$P(\mathfrak{t}, Z) = Z^6 - r_1 Z^4 + r_1 Z^3 + r_0 Z^2 - 2r_0 Z + r_0$$

where r_1 and r_0 are rational functions in $k(\mathfrak{t})$ such that

$$r_1 = \frac{t_1 t_2 (2(t_1 + t_2) - 27)}{(t_1 - t_2)^2}, \quad r_0 = \frac{t_1^2 t_2^2}{(t_1 - t_2)^2}.$$

Let b_1 and b_2 be two elements in an extension K of k such that $b_1 b_2 (4b_1 - 27)(4b_2 - 27)(4b_1 b_2 - 27(b_1 + b_2))(b_1 - b_2) \neq 0$. Let M_i denote the minimal splitting fields of $g(b_i, Y)$ over K and put $n_i = [M_i : K]$, respectively. When a polynomial $F \in K[X]$ over K satisfies $F = \prod_{j=1}^{r} F_j$ for irreducible polynomials F_j over K of degree d_j with $1 \leq d_1 \leq d_2 \leq \cdots \leq d_r$, we say that the decomposition type $\mathcal{DT}_K F$ of F over K is $[d_1, d_2, \ldots, d_r]$.

Theorem 1.1 (Proposition 3.2)**.** *We assume* $n_1 \le n_2$.

(1) *If* $n_1 = 1$*, then* $M_1 \subseteq M_2$ *and* $\mathcal{DT}_K P(\mathfrak{b}, Z) = [n_2, n_2, \ldots, n_2]$.

(2) *When* $n_1 = n_2 = 2$*, we have*

$$\mathcal{DT}_K P(\mathfrak{b}, Z) = \begin{cases} [1,1,2,2] & \text{if and only if } M_1 = M_2, \\ [2,4] & \text{if and only if } M_1 \neq M_2. \end{cases}$$

(3) *If* $n_1 = 2$ *and* $n_2 = 3$*, then* $M_1 \cap M_2 = K$ *and* $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$.

(4) *When* $n_1 = 2$ *and* $n_2 = 6$*, we have*

$$\mathcal{DT}_K P(\mathfrak{b}, Z) = \begin{cases} [3,3] & \text{if and only if } M_1 \subset M_2, \\ [6] & \text{if and only if } M_1 \not\subset M_2. \end{cases}$$

(5) *When* $n_1 = n_2 = 3$*, we have*

$$\mathcal{DT}_K P(\mathfrak{b}, Z) = \begin{cases} [1,1,1,3] & \text{if and only if } M_1 = M_2, \\ [3,3] & \text{if and only if } M_1 \neq M_2. \end{cases}$$

(6) *If* $n_1 = 3$ *and* $n_2 = 6$*, then* $M_1 \cap M_2 = K$ *and* $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$.

(7) *When* $n_1 = n_2 = 6$*, we have*

$$\mathcal{DT}_K P(\mathfrak{b}, Z) = \begin{cases} [1,2,3] & \text{if and only if } M_1 = M_2, \\ [3,3] & \text{if and only if } [M_1 \cap M_2 : K] = 2, \\ [6] & \text{if and only if } M_1 \cap M_2 = K. \end{cases}$$

Corollary 1.2. *With the same notation as in Theorem* 1.1*, the equation* $M_1 = M_2$ *holds if and only if* $P(\mathfrak{b}, Z)$ *has a solution in* K.

Proposition 1.3 (Corollary 2.7)**.** *The sextic polynomial* $P(\mathfrak{t}, Z)$ *is generic for* $(\mathfrak{S}_3)^2$ *over* k.

The exceptional case that $b_1 b_2 (4b_1 - 27)(4b_2 - 27)(4b_1 b_2 - 27(b_1 + b_2))(b_1 - b_2) = 0$ is as follows.

Lemma 1.4 (Lemma 3.8)**.** *We have* $M_i = K$ *if* $b_i(4b_i - 27) = 0$*. When* $(4b_1 b_2 - 27(b_1 + b_2))(b_1 - b_2) = 0$*, it holds that* $M_1 = M_2$.

Remark 1.5. By using an other method with the representation of a cubic field embedding in the ring of 3×3 matrices over $\mathbb{Q}$, Miyake [**6**] gave a solution for the isomorphism problem of $g(t, Y)$ over $\mathbb{Q}$, that is, a condition so that $\mathrm{Spl}_{\mathbb{Q}} g(b_1, Y) = \mathrm{Spl}_{\mathbb{Q}} g(b_2, Y)$ for $b_1, b_2 \in \mathbb{Q}$. His result is one of the motivations of this paper.

In § 2 we recall the notion on the genericity of a regular polynomial and introduce the subfield problem of the polynomial. We show the genericity of $P(\mathfrak{t},Z)$ for $(\mathfrak{S}_3)^2$ over k (Proposition 1.3). In § 3 we study the specialization of $P(\mathfrak{t},Z)$ and solve the subfield problem of $g(t,Y)$ (Theorem 1.1). In § 4 we exhibit the discriminants of the polynomials described in § 2. In § 5 we study the descent genericity of $P(\mathfrak{t},Z)$ and present explicit generic polynomials $P_H(\mathfrak{c},Z)$ for all subgroups H of $(\mathfrak{S}_3)^2$ as degenerations of $P(\mathfrak{t},Z)$.

Acknowledgement. The author is supported by the 21st Century COE Program "Development of Dynamic Mathematics with High Functionality".

§ 2. Genericity of the sextic polynomial

We first recall the notion on the genericity of a regular polynomial (cf. Jensen-Ledet-Yui [**3**]) and introduce the subfield problem of the polynomial. Let k be a field and G a finite group. The rational function field $k(t_1,t_2,\ldots,t_m)$ over k with m variables $t_1,t_2,\ldots,t_m$ is denoted by $k(\mathfrak{t})$ where $\mathfrak{t}=(t_1,t_2,\ldots,t_m)$. For a polynomial $F(X)\in K[X]$ over a field K let us denote by $\mathrm{Spl}_K F(X)$ the minimal splitting field of $F(X)$ over K. We say a polynomial $F(\mathfrak{t},X)\in k(\mathfrak{t})[X]$ is a k-regular G-polynomial or a regular polynomial over k for G if $L=\mathrm{Spl}_{k(\mathfrak{t})}F(\mathfrak{t},X)$ is a Galois extension with $\mathrm{Gal}(L/k(\mathfrak{t}))\simeq G$ and $L\cap\overline{k}=k$ where $\overline{k}$ is an algebraic closure of k. For example, if n is a positive integer greater than 2, then the Kummer polynomial $X^n-t\in\mathbb{Q}(t)[X]$ is a regular polynomial for the cyclic group $\mathcal{C}_n$ of order n not over $\mathbb{Q}$ but over $\mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n-th root of unity in $\overline{\mathbb{Q}}$. A k-regular G-polynomial $F(\mathfrak{t},X)\in k(\mathfrak{t})[X]$ is called to be generic over k if $F(\mathfrak{t},X)$ yields all the Galois G-extensions containing k, that is, for every Galois extension L/K with $\mathrm{Gal}(L/K)\simeq G$ and $K\supseteq k$ there exists a K-specialization $\mathfrak{a}=(a_1,a_2,\ldots,a_m)$, $a_i\in K$ so that $L=\mathrm{Spl}_K F(\mathfrak{a},X)$. The subfield problem for a regular polynomial $F(\mathfrak{t},X)$ is to determine in terms of $\mathfrak{a}=(a_1,a_2,\ldots,a_m)$ and $\mathfrak{b}=(b_1,b_2,\ldots,b_m)$ whether $\mathrm{Spl}_K F(\mathfrak{a},X)\subseteq\mathrm{Spl}_K F(\mathfrak{b},X)$ or not.

In the following we construct the sextic polynomial $P(\mathfrak{t},Z)$ and show the genericity of $P(\mathfrak{t},Z)$. Let k be a field with $\mathrm{char}(k)\neq 2,3$ and $k(s)$ the rational function field over k in one variable s. Let $f(s,X)$ be a cubic polynomial over $k(s)$ of the form

$$f(s,X) = X^3 - 3sX^2 - (3s+3)X - 1 = X^3 - 3X - 1 - 3s(X^2+X),$$

which is called the simplest cubic polynomial of Shanks type [**10**]. It is known that $f(s,X)$ is generic for $\mathcal{C}_3$ over k (cf. [**9**]). Let $A_2(X)$ and $A_3(X)$ be linear fractionals over k such that $A_2(X) = -X-1$ and $A_3(X) = -(X+1)/X$. Then one has $A_2^2(X) = A_3^3(X) = X$. It is easy to check

Lemma 2.1. *We have $f(A_2(s),X) = -f(s,A_2(X))$. Every solution $x \in \overline{k(s)}$ of $f(s,X)=0$ satisfies that $f(s,X) = (X-x)(X-A_3(x))(X-A_3^2(x))$.*

Let us recall a descent Kummer theory studied in a previous paper [**5**] (see also Morton [**7**], Chapman [**1**] and Ogawa [**8**]). Let $+_T$ be a composite law on $T = \mathbb{P}^1 - \{\zeta, \zeta^{-1}\}$ such that $a_1 +_T a_2 = (a_1a_2-1)/(a_1+a_2+1)$ for $a_1, a_2 \in T$ where ζ is a primitive third root of unity in $\overline{k}$. Then T is an abelian group with $+_T$. In fact, T is an algebraic torus of dimension 1 with group isomorphism $\varphi : T \to \mathbb{G}_m$, $a \mapsto (a-\zeta)/(a-\zeta^{-1})$ over $k(\zeta)$. The composite law $+_T$ satisfies $a_1 +_T a_2 = \varphi^{-1}(\varphi(a_1)\varphi(a_2))$. The identity 0_T of T is $\infty = \varphi^{-1}(1)$. The inverse $-_T a$ of $a \in T$ is equal to $-a-1$. The 3-torsion subgroup $T[3] = \mathrm{Ker}([3] : T \to T)$ of T is generated by $-1 = \varphi^{-1}(\zeta)$ where $[n]$ is the multiplication by n map on T. For an $x \in \overline{k(s)}$ the equation $f(s,x) = 0$ holds if and only if $[3](x) = s$. Thus the subfield problem of $f(s,X)$ can be solved by the cohomological argument related to the group T (see [**5**]). One can consider the functions $A_2(X)$ and $A_3(X)$ as $A_2(X) = -_T X$ and $A_3(X) = X +_T (-1)$, respectively. Lemma 2.1 implies

Corollary 2.2. *We have*

$$f(s,X)f(-_T s, X) = (X^2+X+1)^3 - 9(s^2+s+1)(X^2+X)^2,$$

whose zero set is equal to

$$\begin{aligned}\mathcal{A}(x) &= \{x, A_3(x), A_3^2(x), A_2(x), A_3A_2(x), A_3^2A_2(x)\}\\ &= \left\{x, -\frac{x+1}{x}, -\frac{1}{x+1}, -x-1, -\frac{x}{x+1}, \frac{1}{x}\right\}\end{aligned}$$

for a solution $x \in \overline{k(s)}$ of $f(s,X) = 0$.

Let $g(t,Y)$ be as in Introduction and $\delta \in \overline{k(t)}$ a square root of the discriminant of the polynomial $g(t,Y)$, that is,

$$g(t,Y) = Y^3 - tY - t = Y^3 - t(Y+1)$$

and $\delta^2 = 4t^3 - 27t^2$. It is known that $g(t,Y)$ is generic for $\mathfrak{S}_3$ over k (cf. [**9**]).

Lemma 2.3. *If s and t have a relation $s = (9t-\delta)/(2\delta) \in k(t,\delta)$, then*

$$\mathrm{Spl}_{k(t)} g(t,Y) = \mathrm{Spl}_{k(t,\delta)} f(s,X) = k(t,x)$$

for a solution $x \in \overline{k(t)}$ of $f(s,X) = 0$. The Galois group $\mathrm{Gal}(k(t,x)/k(t))$ *is equal to $\langle \sigma, \tau \rangle \simeq \mathfrak{S}_3$ where σ and $\tau \in \mathrm{Gal}(k(t,x)/k(t))$ satisfy $\sigma(x) = x +_T (-1)$ and $\tau(x) = -_T x$, respectively.*

Proof. For $s = (9t-\delta)/(2\delta)$ and $\gamma = 3t/\delta \in k(t,\delta)$, one can see that $f(s, \gamma Y + s) = \gamma^3 g(t,Y)$. This means that $\mathrm{Spl}_{k(t,\delta)} g(t,Y) = \mathrm{Spl}_{k(t,\delta)} f(s,X)$. Note that $\delta = \pm(y_1 - y_2)(y_2 - y_3)(y_3 - y_1) \in \mathrm{Spl}_{k(t)} g(t,Y)$ where $g(t,Y) = \prod_{i=1}^{3}(Y - y_i)$ for $y_i \in \overline{k(t)}$. Thus we have $\mathrm{Spl}_{k(t)} g(t,Y) = \mathrm{Spl}_{k(t,\delta)} g(t,Y) = \mathrm{Spl}_{k(t,\delta)} f(s,X)$. Lemma 2.1 implies that $\mathrm{Spl}_{k(t,\delta)} f(s,X) = k(t,\delta,x)$. Since $s = [3]x \in k(x)$ and $\delta = 9t/(2s+1) \in k(t,x)$, we have $k(t,\delta,x) = k(t,x)$. Here $g(t,Y)$ is a cubic Eisenstein polynomial at the prime divisor t and the discriminant δ^2 of $g(t,Y)$ is not square in $k(t)$. Thus it holds that $[k(t,x) : k(t)] = [\mathrm{Spl}_{k(t)} g(t,Y) : k(t)] = 6$. The element x is a zero of $f(s,X) f(-_T s, X) = (X^2 + X + 1)^3 - 27t(X^2+X)^2/(4t-27)$ which is defined over $k(t)$. This means that $f(s,X) f(-_T s, X)$ is the minimal polynomial of x over $k(t)$. Corollary 2.2 implies that there exist elements σ and τ in $\mathrm{Gal}(k(t,x)/k(t))$ such that $\sigma(x) = A_3(x)$ and $\tau(x) = A_2(x)$. Since the set $\{\sigma^i \tau^j (x) | i,j \in \mathbb{Z}\} = \mathcal{A}(x)$ has order 6, so does the subgroup $\langle \sigma, \tau \rangle$ of $\mathrm{Gal}(k(t,x)/k(t))$. Hence we have $\mathrm{Gal}(k(t,x)/k(t)) = \langle \sigma, \tau \rangle \simeq \mathfrak{S}_3$. $\square$

Let $P(\mathfrak{t}, Z) \in k(\mathfrak{t})[Z]$ be the sextic polynomial as in Introduction, i.e.,

$$P(\mathfrak{t}, Z) = Z^6 - r_1 Z^4 + r_1 Z^3 + r_0 Z^2 - 2r_0 Z + r_0$$

where $r_1 = t_1 t_2 (2(t_1 + t_2) - 27)/(t_1 - t_2)^2$ and $r_0 = t_1^2 t_2^2/(t_1 - t_2)^2$.

Proposition 2.4. *We have* $\mathrm{Spl}_{k(\mathfrak{t})} P(\mathfrak{t}, Z) = \mathrm{Spl}_{k(\mathfrak{t})} g(t_1, Y) \cdot \mathrm{Spl}_{k(\mathfrak{t})} g(t_2, Y)$.

For $i = 1$ and 2 let δ_i be square roots of $4t_i^3 - 27t_i^2$ in $\overline{k(\mathfrak{t})}$ and put $s_i = (9t_i - \delta_i)/(2\delta_i)$, respectively. Let us define $s_\pm = s_1 \pm_T s_2$ and $u_\pm = 9(s_\pm^2 + s_\pm + 1)$, respectively.

Lemma 2.5. *We have*

$$
\begin{aligned}
s_\pm &= \frac{27t_1t_2 - 3(\delta_1 t_2 \pm \delta_2 t_1) \mp \delta_1\delta_2}{6(\delta_1 t_2 \pm \delta_2 t_1)}, \\
u_\pm &= \frac{t_1t_2(2(t_1+t_2) - 27) \mp \delta_1\delta_2}{2(t_1 - t_2)^2},
\end{aligned}
$$

$u_+ + u_- = r_1$ *and* $u_+u_- = r_0$.

Proof. It follows from the definition that

$$
\begin{aligned}
s_+ &= \frac{(\frac{9t_1 - \delta_1}{2\delta_1})(\frac{9t_2 - \delta_2}{2\delta_2}) - 1}{\frac{9t_1 - \delta_1}{2\delta_1} + \frac{9t_2 - \delta_2}{2\delta_2} + 1} \\
&= \frac{(9t_1 - \delta_1)(9t_2 - \delta_2) - 4\delta_1\delta_2}{18(\delta_1 t_2 + \delta_2 t_1)} \\
&= \frac{27t_1t_2 - 3(\delta_1 t_2 + \delta_2 t_1) - \delta_1\delta_2}{6(\delta_1 t_2 + \delta_2 t_1)}.
\end{aligned}
$$

Then one has

$$
\begin{aligned}
u_+ &= 9((s_+ + 1/2)^2 + 3/4) \\
&= (\frac{27t_1t_2 - \delta_1\delta_2}{2(\delta_1 t_2 + \delta_2 t_1)})^2 + \frac{27}{4} \\
&= \frac{(27t_1t_2 - \delta_1\delta_2)^2 + 27(\delta_1 t_2 + \delta_2 t_1)^2}{4(\delta_1 t_2 + \delta_2 t_1)^2} \\
&= \frac{(27t_1^2 + \delta_1^2)(27t_2^2 + \delta_2^2)}{4(\delta_1 t_2 + \delta_2 t_1)^2} \\
&= \frac{4t_1^3t_2^3}{(\delta_1 t_2 + \delta_2 t_1)^2} \\
&= \frac{4t_1^3t_2^3(\delta_1 t_2 - \delta_2 t_1)^2}{(\delta_1^2 t_2^2 - \delta_2^2 t_1^2)^2} \\
&= \frac{4t_1^3t_2^3(4t_1^3t_2^2 + 4_2^3t_1^2 - 54t_1^2t_2^2 - 2\delta_1\delta_2 t_1 t_2)}{16(t_1^3t_2^2 - t_2^3t_1^2)^2} \\
&= \frac{t_1t_2(2(t_1+t_2) - 27) - \delta_1\delta_2}{2(t_1 - t_2)^2}.
\end{aligned}
$$

Note that $-_T s_2 = -(9t_2 - \delta_2)/(2\delta_2) - 1 = (9t_2 - \delta_2')/(2\delta_2')$ where $\delta_2' = -\delta_2$. This means that s_- and u_- are obtained from s_+ and u_+ with substituting $-\delta_2$ in δ_2, respectively. Here it holds that $u_+ + u_- = r_1$. By the argument above we have

$$\begin{aligned} u_+u_- &= \frac{4t_1^3t_2^3}{(\delta_1 t_2 + \delta_2 t_1)^2}\frac{4t_1^3t_2^3}{(\delta_1 t_2 - \delta_2 t_1)^2} \\ &= \frac{16t_1^6t_2^6}{16(t_1^3t_2^2 - t_2^3t_1^2)^2} \\ &= \frac{t_1^2t_2^2}{(t_1-t_2)^2}. \quad \square \end{aligned}$$

Let x_i be solutions of $f(s_i, X) = 0$ in $\overline{k(\mathfrak{t})}$, respectively. Let us denote the field $k(\mathfrak{t}, x_1, x_2)$ by L. We define an element $\xi(i_1, i_2, i) \in L$ by

$$\xi(i_1, i_2, i) = [i_1]x_1 +_T [i_2]x_2 +_T [i](-1)$$

for integers i_1, i_2 and $i \in \mathbb{Z}$. Here -1 is a non-trivial 3-torsion element in T. Let Λ be a finite set consisting of elements $\xi(i_1, i_2, i) \in L$ with $i_1, i_2 \in \{\pm 1\}$ and $i \in \{0, 1, 2\}$. We denote by $\beta(X)$ a rational function $(X^2+X+1)/(X^2+X) \in k(X)$. For $j = 1, 2, \ldots, 6$ let $z_j \in \beta(\Lambda)$ be elements in L defined by

$$\begin{aligned} &z_1 = \beta(\xi(1,1,0)), \quad &z_2 = \beta(\xi(1,1,1)), \quad &z_3 = \beta(\xi(1,1,2)), \\ &z_4 = \beta(\xi(1,-1,0)), \quad &z_5 = \beta(\xi(1,-1,1)), \quad &z_6 = \beta(\xi(1,-1,2)). \end{aligned}$$

Lemma 2.6. *We have* $P(\mathfrak{t}, Z) = \prod_{j=1}^{6}(Z - z_j)$.

Proof. Let us assume that $\xi(i_1, i_2, i) = \xi(i_1', i_2', i')$ for integers i_1, i_2, i, i_1', i_2' and $i' \in \mathbb{Z}$. Then it holds that $[i_1]s_1 +_T [i_2]s_2 = [i_1']s_1 +_T [i_2']s_2$ for $[3]\xi(i_1, i_2, i) = [i_1]s_1 +_T [i_2]s_2$. The elements s_1 and s_2 are linearly independent in the group $T(k(\mathfrak{t}, s_1, s_2))$, which means that $(i_1, i_2) = (i_1', i_2')$. Since -1 is a non-trivial 3-torsion, one has $i \equiv i'$ (mod 3). Thus the set Λ has 12 elements. The elements ξ_1 and $\xi_2 \in \Lambda$ satisfy $\beta(\xi_1) = \beta(\xi_2)$ if and only if ξ_1 is equal to ξ_2 or $-_T\xi_2$. This shows that z_j are distinct from each other. For $[3]\xi(i_1, i_2, i) = [i_1]s_1 +_T [i_2]s_2$ the element $\xi(i_1, i_2, i)$ is a solution of $f([i_1]s_1 +_T [i_2]s_2, X) = 0$. Thus one has

$$\begin{aligned} &\textstyle\prod_{\xi \in \Lambda}(X - \xi) \\ &= f(s_1 +_T s_2, X) f(s_1 -_T s_2, X) f(-_T s_1 +_T s_2, X) f(-_T s_1 -_T s_2, X) \\ &= f(s_+, X) f(-_T s_+, X) f(s_-, X) f(-_T s_-, X) \\ &= ((X^2+X+1)^3 - u_+(X^2+X)^2)((X^2+X+1)^3 - u_-(X^2+X)^2) \\ &= (X^2+X+1)^6 - r_1(X^2+X+1)^3(X^2+X)^2 + r_0(X^2+X)^4, \end{aligned}$$

which is equal to $P(\mathfrak{t}, \beta(X))(X^2+X)^6$. This implies that z_j are solutions of $P(\mathfrak{t}, Z) = 0$. Since z_j are distinct, we have $P(\mathfrak{t}, Z) = \prod_{j=1}^{6}(Z - z_j)$. $\square$

Proof of Proposition 2.4. Lemma 2.3 implies that $L = k(\mathfrak{t}, x_1, x_2)$ is equal to the composite field $\mathrm{Spl}_{k(\mathfrak{t})} g(t_1, Y) \mathrm{Spl}_{k(\mathfrak{t})} g(t_2, Y)$ of two extensions $\mathrm{Spl}_{k(\mathfrak{t})} g(t_1, Y)$ and $\mathrm{Spl}_{k(\mathfrak{t})} g(t_2, Y)$ over $k(\mathfrak{t})$. Let G be the Galois group $\mathrm{Gal}(L/k(\mathfrak{t}))$. Lemma 2.3 means that there exist elements $\sigma_1, \tau_1, \sigma_2$ and τ_2 in G such that

$$\begin{array}{llll} \sigma_1(x_1) = x_1 +_T (-1), & \tau_1(x_1) = -_T x_1, & \sigma_2(x_1) = x_1, & \tau_2(x_1) = x_1, \\ \sigma_1(x_2) = x_2, & \tau_1(x_2) = x_2, & \sigma_2(x_2) = x_2 +_T (-1), & \tau_2(x_2) = -_T x_2. \end{array}$$

Then it holds that $G = \langle \sigma_1, \tau_1, \sigma_2, \tau_2 \rangle = \langle \sigma_1, \tau_1 \rangle \times \langle \sigma_2, \tau_2 \rangle \simeq (\mathfrak{S}_3)^2$. It follows from the definition that $z_j \in L$. One can calculate $\sigma_1(z_1) = \sigma_1(\beta(\xi(1,1,0))) = \beta(\sigma_1(\xi(1,1,0))) = \beta(\xi(1,1,1)) = z_2$. In the same way as above we see the actions on z_j of some elements in G as follows:

	z_1	z_2	z_3	z_4	z_5	z_6
σ_1	z_2	z_3	z_1	z_5	z_6	z_4
τ_1	z_4	z_6	z_5	z_1	z_3	z_2
σ_2	z_2	z_3	z_1	z_6	z_4	z_5
τ_2	z_4	z_5	z_6	z_1	z_2	z_3

The elements $\rho(z_j)$ for $\rho \in G$ and $z_j \in L$ are denoted at the (ρ, z_j)-components in the table above, respectively. Note that for each z_j there exists an element $\rho \in G$ such that $z_j = \rho(z_1)$. Let G_j be the stabilizer of z_j in G, that is, $G_j = \{\rho \in G | \rho(z_j) = z_j\}$. Then it holds that $G_1 = \langle \sigma_1 \sigma_2^2, \tau_1 \tau_2 \rangle \simeq \mathfrak{S}_3$. It is seen that $G_j = \rho G_1 \rho^{-1} \simeq G_1$ if $z_j = \rho(z_1)$ for $\rho \in G$. Here one has the sequence of the extension fields $L/L^{G_j}/k(\mathfrak{t}, z_j)/k(\mathfrak{t})$. By considering the orders of the Galois groups we have $[L : k(\mathfrak{t})] = 36$ and $[L : L^{G_j}] = 6$. Since z_j are conjugate to each other over $k(\mathfrak{t})$, the degrees $[k(\mathfrak{t}, z_j) : k(\mathfrak{t})]$ are equal to 6. This shows that $L^{G_j} = k(\mathfrak{t}, z_j)$ for every j. It satisfies that $G_1 \cap G_2 = \langle \sigma_1 \sigma_2^2 \rangle \simeq \mathcal{C}_3$, $G_1 \cap G_4 = \langle \tau_1 \tau_2 \rangle \simeq \mathcal{C}_2$ and $G_1 \cap G_2 \cap G_4 = \{1\}$. This implies that $L = L^{G_1 \cap G_2 \cap G_4} = k(\mathfrak{t}, z_1, z_2, z_4)$. Hence we conclude $L = \mathrm{Spl}_{k(\mathfrak{t})} P(\mathfrak{t}, Z)$. □

Proposition 2.4 and the genericity of $g(t, Y)$ imply

Corollary 2.7 (Proposition 1.3)**.** *The polynomial $P(\mathfrak{t}, Z)$ is generic for $(\mathfrak{S}_3)^2$ over k.*

§ 3. Solution of the subfield problem on the generic cubic polynomial

In this section we solve the subfield problem of the cubic polynomial $g(t, Y)$ by using the sextic polynomial $P(\mathfrak{t}, Z)$.

Let $b \in K$ be an element in an extension K of k with $b(4b-27) \neq 0$. Let δ be a square root of $4b^3 - 27b^2$ in $\overline{K}$ and put $a = (9b - \delta)/(2\delta) \in K(\delta)$. Let $Q_b(K)$ be the set of solutions $w \in K$ of the quadratic equation $W^2 = 4b^3 - 27b^2$ and $C_b(K)$ that of the cubic one $g(b, Y) = 0$.

Lemma 3.1. *For a solution $x \in \overline{K}$ of $f(a, X) = 0$, we have $\mathrm{Spl}_K g(b, Y) = K(x)$ and*

$$\mathrm{Gal}(K(x)/K) = \begin{cases} \langle \sigma, \tau \rangle & \simeq \mathfrak{S}_3 \quad \textit{if } Q_b(K) = \emptyset \textit{ and } C_b(K) = \emptyset, \\ \langle \sigma \rangle & \simeq \mathcal{C}_3 \quad \textit{if } Q_b(K) \neq \emptyset \textit{ and } C_b(K) = \emptyset, \\ \langle \iota \rangle & \simeq \mathcal{C}_2 \quad \textit{if } Q_b(K) = \emptyset \textit{ and } C_b(K) \neq \emptyset, \\ \{1\} & \qquad\quad \textit{otherwise}, \end{cases}$$

where $\sigma(x) = A_3(x) = x +_T (-1)$, $\tau(x) = A_2(x) = -_T x$ and $\iota(x) = A_3^i A_2(x)$ for an integer $i \in \mathbb{Z}$.

Proof. In the same way as in the proof of Lemma 2.3 one sees $\mathrm{Spl}_K g(b, Y) = K(x)$. Let G_0 be the Galois group $\mathrm{Gal}(K(x)/K)$. Since $g(b, Y)$ is cubic, G_0 is isomorphic to a subgroup of $\mathfrak{S}_3$. The sets $Q_b(K)$ (resp. $C_b(K)$) are empty if and only if G_0 contains subgroups which are isomorphic to the cyclic groups $\mathcal{C}_2$ (resp. $\mathcal{C}_3$). It determines the group structure of G_0 completely. Let $G_0(x)$ be the orbit of x by G_0, that is, $G_0(x) = \{\rho(x) | \rho \in G_0\}$. Note that x is a solution of $f(a, X) f(-_T a, X) = 0$ which is a equation over K. Thus $G_0(x)$ has elements as those of $\mathcal{A}(x)$ at Corollary 2.2. If $G_0 \simeq \mathfrak{S}_3$, then $G_0(x)$ is the same form as $\mathcal{A}(x)$, whose order is equal to 6. Thus one has $G_0 = \langle \sigma, \tau \rangle$. When $G_0 \simeq \mathcal{C}_3$, the set $G_0(x)$ has three elements. Note that $A_2(X)$, $A_3 A_2(X)$ and $A_3^2 A_2(X)$ are linear fractionals of period 2. Thus we have $G_0(x) = \{x, A_3(x), A_3^2(x)\}$, which means that $G_0 = \langle \sigma \rangle$. If $G_0 \simeq \mathcal{C}_2$, then $G_0 = \langle \iota \rangle$ where $\iota(x) = A_3^i A_2(x)$ for an integer $i \in \mathbb{Z}$. The integer i depends on the choice of the solution x. In fact, if x satisfies $\iota(x) = A_3^i A_2(x)$ for an integer $i \in \mathbb{Z}$, then $x' = A_3^i(x)$ is a solution of $f(a, X) = 0$ such that $\iota(x') = A_2(x')$. It is obvious for the case $G_0 = \{1\}$. □

Let $F \in K[X]$ be a polynomial over K and $d_1 \leq d_2 \leq \cdots \leq d_r$ positive integers. If there exist irreducible polynomials F_j over K of degree d_j such that $F = \prod_{j=1}^r F_j$, then we say that the decomposition type of F over K is $[d_1, d_2, \ldots, d_r]$ and denote it by $\mathcal{DT}_K F$. Let b_1 and b_2 be two elements in K such that $b_1 b_2 (4b_1 - 27)(4b_2 -$

$27)(4b_1b_2-27(b_1+b_2))(b_1-b_2)\neq 0$. Now put $M_i=\mathrm{Spl}_K g(b_i,Y)$ and $n_i=[M_i:K]$, respectively. One can calculate the integers n_i by using Lemma 3.1. We obtain a criterion whether $M_1\subseteq M_2$ or not in terms of the decomposition type $\mathcal{DT}_K P(\mathfrak{b},Z)$ of $P(\mathfrak{b},Z)$ over K for $\mathfrak{b}=(b_1,b_2)$ as follows.

Proposition 3.2 (Theorem 1.1)**.** *We assume $n_1\leq n_2$.*

(1) *If $n_1=1$, then $M_1\subseteq M_2$ and $\mathcal{DT}_K P(\mathfrak{b},Z)=[n_2,n_2,\ldots,n_2]$.*

(2) *When $n_1=n_2=2$, we have*

$$\mathcal{DT}_K P(\mathfrak{b},Z)=\begin{cases}[1,1,2,2] & \text{if } M_1=M_2,\\ [2,4] & \text{otherwise.}\end{cases}$$

(3) *If $n_1=2$ and $n_2=3$, then $M_1\cap M_2=K$ and $\mathcal{DT}_K P(\mathfrak{b},Z)=[6]$.*

(4) *When $n_1=2$ and $n_2=6$, we have*

$$\mathcal{DT}_K P(\mathfrak{b},Z)=\begin{cases}[3,3] & \text{if } M_1\subset M_2,\\ [6] & \text{otherwise.}\end{cases}$$

(5) *When $n_1=n_2=3$, we have*

$$\mathcal{DT}_K P(\mathfrak{b},Z)=\begin{cases}[1,1,1,3] & \text{if } M_1=M_2,\\ [3,3] & \text{otherwise.}\end{cases}$$

(6) *If $n_1=3$ and $n_2=6$, then $M_1\cap M_2=K$ and $\mathcal{DT}_K P(\mathfrak{b},Z)=[6]$.*

(7) *When $n_1=n_2=6$, we have*

$$\mathcal{DT}_K P(\mathfrak{b},Z)=\begin{cases}[1,2,3] & \text{if } M_1=M_2,\\ [3,3] & \text{if } [M_1\cap M_2:K]=2,\\ [6] & \text{otherwise.}\end{cases}$$

Let L be the composite field M_1M_2 and G the Galois group $\mathrm{Gal}(L/K)$. For $i=1$ and 2 let δ_i be square roots of $4b_i^3-27b_i^2$ in $\overline{K}$ and put $a_i=(9b_i-\delta_i)/(2\delta_i)$, respectively. Let x_i be solutions of $f(a_i,X)=0$ in $\overline{K}$. In the same way as for the case of the function field $k(\mathfrak{t})$ described at the previous section, we define $z_j\in L$ for integers $j=1,2,\ldots,6$. Since $\mathrm{disc}_Z P(\mathfrak{b},Z)$ is not equal to 0 due to Lemma 4.2 below, the elements z_j are distinct from each other.

Lemma 3.3. *If $n_1=1$, then $M_1\subseteq M_2$ and $\mathcal{DT}_K P(\mathfrak{b},Z)=[n_2,n_2,\ldots,n_2]$.*

Proof. When $n_1=n_2=1$, we have $x_1,x_2\in K$ and $z_j\in K$. This means that $\mathcal{DT}_K P(\mathfrak{b},Z)=[1,1,1,1,1,1]$. When $(n_1,n_2)=(1,2)$, we have $G=\langle\iota_2\rangle$ where $\iota_2(x_1)=x_1$ and $\iota_2(x_2)=A_3^iA_2(x_2)$ for an $i\in\mathbb{Z}$. If $\iota_2(x_2)=A_2(x_2)$, then

$$\iota_2: z_1\mapsto z_4\mapsto z_1,\quad z_2\mapsto z_5\mapsto z_2,\quad z_3\mapsto z_6\mapsto z_3,$$

which means that $\mathcal{DT}_K P(\mathfrak{b}, Z) = [2,2,2]$. In the same way as above one sees $\mathcal{DT}_K P(\mathfrak{b}, Z) = [2,2,2]$ provided $\iota_2(x_2) = A_3^i A_2(x_2)$ for every $i \in \mathbb{Z}$. If $(n_1, n_2) = (1,3)$, then $G = \langle \sigma_2 \rangle$ with $\sigma_2(x_1) = x_1$ and $\sigma_2(x_2) = A_3(x_2)$. Then one has

$$\sigma_2 : z_1 \mapsto z_2 \mapsto z_3 \mapsto z_1, \quad z_4 \mapsto z_6 \mapsto z_5 \mapsto z_4,$$

which implies that $\mathcal{DT}_K P(\mathfrak{b}, Z) = [3,3]$. When $(n_1, n_2) = (1,6)$, we have $G = \langle \sigma_2, \tau_2 \rangle$ with $\sigma_2(x_1) = x_1$, $\tau_2(x_1) = x_1$, $\sigma_2(x_2) = A_3(x_2)$ and $\tau_2(x_2) = A_2(x_2)$. Then σ_2 and τ_2 satisfy $\sigma_2 : z_1 \mapsto z_2 \mapsto z_3, z_4 \mapsto z_6 \mapsto z_5$ and $\tau_2(z_1) = z_4$, respectively. Thus we have $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$. □

Lemma 3.4. *Now assume $n_1 = 2$. When $n_2 = 2$, we have*

$$\mathcal{DT}_K P(\mathfrak{b}, Z) = \begin{cases} [1,1,2,2] & \text{if } M_1 = M_2, \\ [2,4] & \text{otherwise.} \end{cases}$$

If $n_2 = 3$, then $M_1 \cap M_2 = K$ and $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$. For the case of $n_2 = 6$ we have

$$\mathcal{DT}_K P(\mathfrak{b}, Z) = \begin{cases} [3,3] & \text{if } M_1 \subset M_2, \\ [6] & \text{otherwise.} \end{cases}$$

Proof. Let us first consider the case that $n_1 = n_2 = 2$ and $M_1 = M_2$. Then it satisfies that $G = \langle \iota \rangle$ where $\iota(x_1) = A_3^{i_1} A_2(x_1)$ and $\iota(x_2) = A_3^{i_2} A_2(x_2)$ for integers $i_1, i_2 \in \mathbb{Z}$. By replacing x_1 and x_2 by the solutions $x_1' = A_3^{i_1}(x_1)$ and $x_2' = A_3^{i_2}(x_1)$, one may have $\iota(x_1') = A_2(x_1')$ and $\iota(x_2') = A_2(x_2')$, respectively. The replacement of (x_1, x_2) by (x_1', x_2') permutes the elements z_j, however, it does not change the polynomial $P(\mathfrak{b}, Z)$ and the decomposition type $\mathcal{DT}_K P(\mathfrak{b}, Z)$. So we may check only the case $i_1 = i_2 = 0$. It holds that

$$\iota : z_1 \mapsto z_1, \quad z_2 \mapsto z_3 \mapsto z_2, \quad z_4 \mapsto z_4, \quad z_5 \mapsto z_6 \mapsto z_5,$$

which means $\mathcal{DT}_K P(\mathfrak{b}, Z) = [1,1,2,2]$. If $n_1 = n_2 = 2$ and $M_1 \neq M_2$, then $G = \langle \iota_1, \iota_2 \rangle$ where $\iota_1(x_1) = A_3^{i_1} A_2(x_1)$, $\iota_1(x_2) = x_2$, $\iota_2(x_1) = x_1$ and $\iota_2(x_2) = A_3^{i_2} A_2(x_2)$ for integers $i_1, i_2 \in \mathbb{Z}$. When $i_1 = i_2 = 0$, it satisfies

$$\begin{aligned} \iota_1 : &\quad z_1 \mapsto z_4 \mapsto z_1, \quad z_2 \mapsto z_6 \mapsto z_2, \quad z_3 \mapsto z_5 \mapsto z_3, \\ \iota_2 : &\quad z_1 \mapsto z_4 \mapsto z_1, \quad z_2 \mapsto z_5 \mapsto z_2, \quad z_3 \mapsto z_6 \mapsto z_3. \end{aligned}$$

This shows that $\mathcal{DT}_K P(\mathfrak{b}, Z) = [2,4]$. If $(n_1, n_2) = (2,3)$, then $G = \langle \iota_1, \sigma_2 \rangle$ where $\iota_1(x_1) = A_3^{i_1} A_2(x_1)$, $\iota_1(x_2) = x_2$, $\sigma_2(x_1) = x_1$ and $\sigma_2(x_2) = A_3(x_2)$ for an integer $i_1 \in \mathbb{Z}$. In the case $i_1 = 0$ one has that $\iota_1(z_1) = z_4$ and $\sigma_2 : z_1 \mapsto z_2 \mapsto z_3, z_4 \mapsto$

$z_6 \mapsto z_5$. Thus we have $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$. Let us assume $(n_1, n_2) = (2, 6)$. If $M_1 \subset M_2$, then $G = \langle \sigma_2, \tau \rangle$ where $\sigma_2(x_1) = x_1$, $\sigma_2(x_2) = A_3(x_2)$, $\tau(x_1) = A_3^{i_1} A_2(x_1)$ and $\tau(x_2) = A_2(x_2)$ for an integer $i_1 \in \mathbb{Z}$. Under the condition $i_1 = 0$ one has

$$\begin{array}{rl} \sigma_2 : & z_1 \mapsto z_2 \mapsto z_3 \mapsto z_1, \quad z_4 \mapsto z_6 \mapsto z_5 \mapsto z_4, \\ \tau : & z_1 \mapsto z_1, \quad z_2 \mapsto z_3 \mapsto z_2, \quad z_4 \mapsto z_4, \quad z_5 \mapsto z_6 \mapsto z_5, \end{array}$$

which means that $\mathcal{DT}_K P(\mathfrak{b}, Z) = [3, 3]$. If $M_1 \not\subset M_2$, then $G = \langle \iota_1, \sigma_2, \tau_2 \rangle$ where $\iota_1(x_1) = A_3^{i_1} A_2(x_1)$, $\iota_1(x_2) = x_2$, $\sigma_2(x_1) = x_1$, $\sigma_2(x_2) = A_3(x_2)$, $\tau_2(x_1) = x_1$ and $\tau_2(x_2) = A_2(x_2)$ for an integer $i_1 \in \mathbb{Z}$. Then in the same way as in the case $(n_1, n_2) = (1, 6)$, one has $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$. □

Lemma 3.5. *Assume* $n_1 = 3$. *When* $n_2 = 3$, *we have*

$$\mathcal{DT}_K P(\mathfrak{b}, Z) = \begin{cases} [1, 1, 1, 3] & \text{if } M_1 = M_2, \\ [3, 3] & \text{otherwise.} \end{cases}$$

If $n_2 = 6$, *then* $M_1 \cap M_2 = K$ *and* $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$.

Proof. Let us assume that $n_1 = n_2 = 3$ and $M_1 = M_2$. Then it holds that $G = \langle \sigma \rangle$ where $\sigma(x_1) = A_3(x_1)$ and $\sigma(x_2) = A_3^i(x_2)$ for $i \in \{1, 2\}$. Here one sees

$$\sigma : \begin{cases} z_1 \mapsto z_3 \mapsto z_2 \mapsto z_1, \quad z_4 \mapsto z_4, \quad z_5 \mapsto z_5, \quad z_6 \mapsto z_6 & \text{if } i = 1, \\ z_1 \mapsto z_1, \quad z_2 \mapsto z_2, \quad z_3 \mapsto z_3, \quad z_4 \mapsto z_6 \mapsto z_5 \mapsto z_4 & \text{if } i = 2. \end{cases}$$

This means that $\mathcal{DT}_K P(\mathfrak{b}, Z) = [1, 1, 1, 3]$. When $n_1 = n_2 = 3$ and $M_1 \neq M_2$, we have $G = \langle \sigma_1, \sigma_2 \rangle$ where $\sigma_1(x_1) = A_3(x_1)$, $\sigma_1(x_2) = x_2$, $\sigma_2(x_1) = x_1$ and $\sigma_2(x_2) = A_3(x_2)$. Then

$$\begin{array}{rl} \sigma_1 : & z_1 \mapsto z_2 \mapsto z_3 \mapsto z_1, \quad z_4 \mapsto z_5 \mapsto z_6 \mapsto z_4, \\ \sigma_2 : & z_1 \mapsto z_2 \mapsto z_3 \mapsto z_1, \quad z_4 \mapsto z_6 \mapsto z_5 \mapsto z_4, \end{array}$$

which implies that $\mathcal{DT}_K P(\mathfrak{b}, Z) = [3, 3]$. If $(n_1, n_2) = (3, 6)$, then $M_1 \cap M_2 = K$ and $G = \langle \sigma_1, \sigma_2, \tau_2 \rangle$ where $\sigma_1(x_1) = A_3(x_1)$, $\sigma_1(x_2) = x_2$, $\sigma_2(x_1) = x_1$, $\sigma_2(x_2) = A_3(x_2)$, $\tau_2(x_1) = x_1$ and $\tau_2(x_2) = A_2(x_2)$. In the same way as in the case $(n_1, n_2) = (1, 6)$, one has $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$. □

Lemma 3.6. *When* $n_1 = n_2 = 6$, *we have*

$$\mathcal{DT}_K P(\mathfrak{b}, Z) = \begin{cases} [1, 2, 3] & \text{if } M_1 = M_2, \\ [3, 3] & \text{if } [M_1 \cap M_2 : K] = 2, \\ [6] & \text{otherwise.} \end{cases}$$

Proof. If $M_1 = M_2$, then $G = \langle \sigma, \tau \rangle$ where $\sigma(x_1) = A_3(x_1)$, $\sigma(x_2) = A_3^i(x_2)$ $\tau(x_1) = A_2(x_1)$ and $\tau(x_2) = A_3^{i_2} A_2(x_2)$ for integers $i \in \{1, 2\}$ and $i_2 \in \mathbb{Z}$. In the case $(i, i_2) = (1, 0)$ we have

$$\begin{array}{ll} \sigma: & z_1 \mapsto z_3 \mapsto z_2 \mapsto z_1, \quad z_4 \mapsto z_4, \quad z_5 \mapsto z_5, \quad z_6 \mapsto z_6, \\ \tau: & z_1 \mapsto z_1, \quad z_2 \mapsto z_3 \mapsto z_2, \quad z_4 \mapsto z_4, \quad z_5 \mapsto z_6 \mapsto z_5. \end{array}$$

This shows that $\mathcal{DT}_K P(\mathfrak{b}, Z) = [1, 2, 3]$. When $[M_1 \cap M_2 : K] = 2$, we have $G = \langle \sigma_1, \sigma_2, \tau \rangle$ where $\sigma_1(x_1) = A_3(x_1)$, $\sigma_1(x_2) = x_2$, $\sigma_2(x_1) = x_1$, $\sigma_2(x_2) = A_3(x_2)$ $\tau(x_1) = A_2(x_1)$ and $\tau(x_2) = A_3^{i_2} A_2(x_2)$ for an integer $i_2 \in \mathbb{Z}$. For the case $i_2 = 0$ one has

$$\begin{array}{ll} \sigma_1: & z_1 \mapsto z_2 \mapsto z_3 \mapsto z_1, \quad z_4 \mapsto z_5 \mapsto z_6 \mapsto z_4, \\ \sigma_2: & z_1 \mapsto z_2 \mapsto z_3 \mapsto z_1, \quad z_4 \mapsto z_6 \mapsto z_5 \mapsto z_4, \\ \tau: & z_1 \mapsto z_1, \quad z_2 \mapsto z_3 \mapsto z_2, \quad z_4 \mapsto z_4, \quad z_5 \mapsto z_6 \mapsto z_5. \end{array}$$

Thus we have $\mathcal{DT}_K P(\mathfrak{b}, Z) = [3, 3]$. If $M_1 \cap M_2 = K$, then $G = \langle \sigma_1, \sigma_2, \tau_1, \tau_2 \rangle$ where $\sigma_1(x_1) = A_3(x_1)$, $\sigma_1(x_2) = x_2$, $\sigma_2(x_1) = x_1$, $\sigma_2(x_2) = A_3(x_2)$, $\tau_1(x_1) = A_2(x_1)$, $\tau_1(x_2) = x_2$, $\tau_2(x_1) = x_1$ and $\tau_2(x_2) = A_2(x_2)$. In the same way as in the case $(n_1, n_2) = (1, 6)$, one has $\mathcal{DT}_K P(\mathfrak{b}, Z) = [6]$. □

Remark 3.7. In the proofs of Lemmas 3.3 to 3.6 one may have $i_1 = i_2 = 0$ by replacing the solutions x_1 and x_2 by others solutions of $f(a_1, Y) = 0$ and $f(a_2, Y) = 0$, respectively. We may have $i = 1$ by replacing the solutions x_2 of $f(a_2, Y) = 0$ by a solution $-_T x_2$ of $f(-_T a_2, Y) = 0$. Such replacements do not change the extensions M_1, M_2, the polynomial $P(\mathfrak{b}, Z)$ and the decomposition type $\mathcal{DT}_K P(\mathfrak{b}, Z)$.

Lemmas 3.3 to 3.6 verify Proposition 3.2.

Proof of Theorem 1.1. For a fixed (n_1, n_2), Proposition 3.2 means that the decomposition types $\mathcal{DT}_K P(\mathfrak{b}, Z)$ are distinct if the relations between M_1 and M_2 are different, which implies that the converses are also true. This shows Theorem 1.1 completely. □

For the exceptional case that $b_1 b_2 (4b_1 - 27)(4b_2 - 27)(4b_1 b_2 - 27(b_1 + b_2))(b_1 - b_2) = 0$ one sees

Lemma 3.8 (Lemma 1.4). *We have $M_i = K$ provided $b_i(4b_i - 27) = 0$. When $(4b_1 b_2 - 27(b_1 + b_2))(b_1 - b_2) = 0$, it holds that $M_1 = M_2$.*

Proof. Since $g(0, Y) = Y^3$ and $g(27/4, Y) = (Y-3)(Y+3/2)^2$, one has $M_i = K$ if $b_i(4b_i - 27) = 0$. Now assume that $b_i(4b_i-27) \neq 0$ and $4b_1b_2 - 27(b_1+b_2) = 0$. Then one has that $\delta_1^2\delta_2^2 = 27^2 b_1^2 b_2^2$ and $K(\delta_1, \delta_2) = K(\delta_1) = K(\delta_2)$. Lemma 2.5 shows that $a_1 +_T a_2 = -1/2$ or $a_1 -_T a_2 = -1/2$. Since $-1/2 = [3](-1/2) \in [3]T(K)$, it holds that $\mathrm{Spl}_{K(\delta_1,\delta_2)} f(a_1, X) = \mathrm{Spl}_{K(\delta_1,\delta_2)} f(a_2, X)$. Lemma 2.3 implies that $M_i = \mathrm{Spl}_{K(\delta_i)} f(a_i, X)$, respectively. Hence we have $M_1 = M_2$. □

§ 4. Discriminants of the polynomials

Let us denote the discriminants of the polynomials $f(s, X)$ and $g(t, Y)$ by $\Delta_f(s)$ and by $\Delta_g(t)$, respectively.

Lemma 4.1. *We have* $\Delta_f(s) = 3^4(s^2+s+1)^2$ *and* $\Delta_g(t) = t^2(4t-27)$. *Under the relations* $s = (9t-\delta)/(2\delta)$ *and* $\delta^2 = 4t^3 - 27t^2$ *one has* $\Delta_f(s) = 3^6t^2/(4t-27)^2$ *and* $\Delta_g(t) = 3^{10}(s^2+s+1)^2/(2s+1)^6$.

Proof. The equations $s = (9t-\delta)/(2\delta)$ and $\delta^2 = 4t^3 - 27t^2$ imply that $t = 3^3(s^2 + s+1)/(2s+1)^2$. This means that $s^2+s+1 = 3t/(4t-27)$. □

Let $\Delta_P(\mathfrak{t})$ be the discriminant of the polynomial $P(\mathfrak{t}, Z)$.

Lemma 4.2. *We have*

$$\Delta_P(\mathfrak{t}) = \frac{t_1^{10}t_2^{10}(4t_1-27)^3(4t_2-27)^3(4t_1t_2-27(t_1+t_2))^2}{(t_1-t_2)^{18}}.$$

Proof. We first note that $P(\mathfrak{t}, -Z) = g(u_+, Z)g(u_-, Z)$ whose discriminant is equal to that of $P(\mathfrak{t}, Z)$. Here the resultant $\mathrm{Res}_Z(g_1(Z), g_2(Z))$ of two polynomials $g_1(Z)$ and $g_2(Z)$ satisfies an equation

$$\mathrm{disc}_Z(g_1(Z)g_2(Z)) = \mathrm{disc}_Z(g_1(Z))\mathrm{disc}_Z(g_2(Z))\mathrm{Res}_Z(g_1(Z), g_2(Z))^2$$

(cf. [**2**] § 3.3). Lemma 2.5 implies that

$$\begin{aligned}&\mathrm{disc}_Z g(u_+, Z)\mathrm{disc}_Z g(u_-, Z)\\ &= (4u_+^3 - 27u_+^2)(4u_-^3 - 27u_-^2)\\ &= r_0^2(16r_0 - 108r_1 + 729)\\ &= t_1^4t_2^4(4t_1t_2 - 27(t_1+t_2))^2/(t_1-t_2)^6.\end{aligned}$$

By the Sylvester's matrix method one can calculate that $\mathrm{Res}_Z(g(u_+, Z), g(u_-, Z))$ is equal to $(u_+ - u_-)^3$. It holds that $(u_+ - u_-)^2 = r_1^2 - 4r_0 = t_1^2t_2^2(4t_1-27)(4t_2 - 27)/(t_1-t_2)^4$. Hence the equation of the assertion follows. □

§ 5. Descent genericity of the sextic polynomial

It is known due to Kemper [**4**] that a generic polynomial for a finite group G over a field k yieds not only all the Galois G-extensions containing k but also all the Galois H-extensions containing k for any subgroups H of G. In this section we give explicit generic polynomials $P_H(\mathfrak{c}, Z)$ for all subgroups H of $(\mathfrak{S}_3)^2$ by the degenerations of the sextic polynomial $P(\mathfrak{t}, Z)$.

Let $\lambda(c)$, $\mu(c)$ and $\nu(c) \in k(c)$ be rational functions over k with one variable c such that

$$\lambda(c) = \frac{3^3(c^2+c+1)}{(2c+1)^2}, \quad \mu(c) = \frac{c^3}{3^2(c-9)^2},$$
$$\nu(s) = \lambda([3](c)) = \mu(\lambda(c)) = \frac{3^3(c^2+c+1)^3}{(c-1)^2(2c+1)^2(c+2)^2},$$

where [3] is the multiplication by 3 map of the group T, that is, $[3](c) = (c^3-3c-1)/(3c^2+3c)$. For subgroups $H = \{1\}$, $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathfrak{S}_3$ of $\mathfrak{S}_3$, we define polynomials $g_H(c, Y) \in k(c)[Y]$ by

$$g_{\{1\}}(c, Y) = g(\nu(c), Y), \quad g_{\mathcal{C}_2}(c, Y) = g(\mu(c), Y), \quad g_{\mathcal{C}_3}(c, Y) = g(\lambda(c), Y)$$

and $g_{\mathfrak{S}_3}(c, Y) = g(c, Y)$, respectively. By the direct calculation one sees

Lemma 5.1. *We have*

$$g_{\{1\}}(c, Y) = (Z - \frac{3(c^2+c+1)}{(c-1)(c+2)})(Z + \frac{3(c^2+c+1)}{(c+2)(2c+1)})(Z + \frac{3(c^2+c+1)}{(c-1)(2c+1)}),$$
$$g_{\mathcal{C}_2}(c, Y) = (Z + \frac{c}{c-9})(Z^2 - \frac{c}{c-9}Z - \frac{c^2}{3^2(c-9)}),$$
$$\mathrm{disc}_Z(g_{\{1\}}(c, Y) = \frac{3^{12}c^2(c+1)^2(c^2+c+1)^6}{(c-1)^6(2c+1)^6(c+2)^6},$$
$$\mathrm{disc}_Z(g_{\mathcal{C}_2}(c, Y)) = \frac{c^6(c-27)^2(4c-27)}{3^6(c-9)^6}, \quad \mathrm{disc}_Z(g_{\mathcal{C}_3}(c, Y)) = \frac{3^{10}(c^2+c+1)^2}{(2c+1)^6}.$$

Corollary 5.2. *For each subgroup $H = \{1\}$, $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathfrak{S}_3$ of $\mathfrak{S}_3$, the polynomial $g_H(c, Y)$ is generic for H over k.*

Proof. Lemma 5.1 means that $\mathrm{Spl}_{k(c)}(g_{\{1\}}(c, Y)) = k(c)$ and $\mathrm{Spl}_{k(c)}(g_{\mathcal{C}_2}(c, Y)) = k(c, \sqrt{4c-27})$. Thus $\mathrm{Spl}_{k(c)}(g_{\{1\}}(c, Y))$ and $\mathrm{Spl}_{k(c)}(g_{\mathcal{C}_2}(c, Y))$ are generic. Lemma 2.3 implies that $\mathrm{Spl}_{k(c)}(g_{\mathcal{C}_3}(c, Y)) = \mathrm{Spl}_{k(c)} f(c, X)$ for $\mathrm{disc}_Z(g_{\mathcal{C}_3}(c, Y)) \in k(c)^2$. Since $f(c, X)$ is generic for $\mathcal{C}_3$ over k, so is $g_{\mathcal{C}_3}(c, Y)$. □

For subgroups H of $(\mathfrak{S}_3)^2$ we define polynomials $P_H(\mathfrak{c}, Z) \in k(\mathfrak{c})[Z]$, $\mathfrak{c} = (c_1, c_2)$ by

$$\begin{array}{ll} P_{\{1\}}(\mathfrak{c}, Z) = P(\nu(c_1), \nu(c_2), Z), & P_{\mathfrak{S}_3}(\mathfrak{c}, Z) = P(\nu(c_1), c_2, Z), \\ P_{\mathcal{C}_2}(\mathfrak{c}, Z) = P(\nu(c_1), \mu(c_2), Z), & P_{(\mathcal{C}_3)^2}(\mathfrak{c}, Z) = P(\lambda(c_1), \lambda(c_2), Z), \\ P_{\mathcal{C}_3}(\mathfrak{c}, Z) = P(\nu(c_1), \lambda(c_2), Z), & P_{\mathcal{C}_2 \times \mathfrak{S}_3}(\mathfrak{c}, Z) = P(\mu(c_1), c_2, Z), \\ P_{(\mathcal{C}_2)^2}(\mathfrak{c}, Z) = P(\mu(c_1), \mu(c_2), Z), & P_{\mathcal{C}_3 \times \mathfrak{S}_3}(\mathfrak{c}, Z) = P(\lambda(c_1), c_2, Z), \\ P_{\mathcal{C}_6}(\mathfrak{c}, Z) = P(\mu(c_1), \lambda(c_2), Z), & P_{(\mathfrak{S}_3)^2}(\mathfrak{c}, Z) = P(c_1, c_2, Z). \end{array}$$

Proposition 2.4 and Corollary 5.2 imply

Corollary 5.3. *For every subgroup H of $(\mathfrak{S}_3)^2$ the polynomial $P_H(\mathfrak{c}, Z)$ is generic for H over k.*

Remark 5.4. We omit the description of the discriminants $\mathrm{disc}_Z P_H(\mathfrak{c}, Z)$ of the polynomials $P_H(\mathfrak{c}, Z) = P(\varepsilon_1(c_1), \varepsilon_2(c_2), Z)$ since $\mathrm{disc}_Z P_H(\mathfrak{c}, Z)$ are equal to $\Delta_P(\varepsilon_1(c_1), \varepsilon_2(c_2))$, respectively.

References

[1] R.J. Chapman, *Automorphism polynomials in cyclic cubic extensions*, J. Number Theory **61** (1996), no. 2, 283–291.

[2] H. Cohen, A course in computational algebraic number theory, Grad. Texts in Math. **138**, 1993.

[3] C.U. Jensen, A. Ledet, N. Yui, Generic polynomials, Math. Sci. Res. Inst. Publ. **45**, 2002.

[4] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), no. 1, 139–141.

[5] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta Math. **114** (2004), no. 3, 265–279.

[6] K. Miyake, a communication note.

[7] P. Morton, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory **49** (1994), no. 2, 183–208.

[8] H. Ogawa, *Quadratic reduction of multiplicative group and its applications*, (Japanese) Algebraic number theory and related topics (Japanese) (Kyoto, 2002). Surikaisekikenkyusho Kokyuroku **1324** (2003), 217–224.

[9] J.P. Serre, Topics in Galois theory, Res. Notes in Math. **1**, 1992.

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

(Toru KOMATSU) Faculty of Mathematics, Kyushu University, 6-10-1 Hakozaki Higashiku, Fukuoka, 812-8581 Japan

E-mail address: `trkomatu@math.kyushu-u.ac.jp`

List of MHF Preprint Series, Kyushu University

21st Century COE Program
Development of Dynamic Mathematics with High Functionality

MHF2003-1 Mitsuhiro T. NAKAO, Kouji HASHIMOTO & Yoshitaka WATANABE
A numerical method to verify the invertibility of linear elliptic operators with applications to nonlinear problems

MHF2003-2 Masahisa TABATA & Daisuke TAGAMI
Error estimates of finite element methods for nonstationary thermal convection problems with temperature-dependent coefficients

MHF2003-3 Tomohiro ANDO, Sadanori KONISHI & Seiya IMOTO
Adaptive learning machines for nonlinear classification and Bayesian information criteria

MHF2003-4 Kazuhiro YOKOYAMA
On systems of algebraic equations with parametric exponents

MHF2003-5 Masao ISHIKAWA & Masato WAKAYAMA
Applications of Minor Summation Formulas III, Plücker relations, Lattice paths and Pfaffian identities

MHF2003-6 Atsushi SUZUKI & Masahisa TABATA
Finite element matrices in congruent subdomains and their effective use for large-scale computations

MHF2003-7 Setsuo TANIGUCHI
Stochastic oscillatory integrals - asymptotic and exact expressions for quadratic phase functions -

MHF2003-8 Shoki MIYAMOTO & Atsushi YOSHIKAWA
Computable sequences in the Sobolev spaces

MHF2003-9 Toru FUJII & Takashi YANAGAWA
Wavelet based estimate for non-linear and non-stationary auto-regressive model

MHF2003-10 Atsushi YOSHIKAWA
Maple and wave-front tracking — an experiment

MHF2003-11 Masanobu KANEKO
On the local factor of the zeta function of quadratic orders

MHF2003-12 Hidefumi KAWASAKI
Conjugate-set game for a nonlinear programming problem

MHF2004-1 Koji YONEMOTO & Takashi YANAGAWA
Estimating the Lyapunov exponent from chaotic time series with dynamic noise

MHF2004-2 Rui YAMAGUCHI, Eiko TSUCHIYA & Tomoyuki HIGUCHI
State space modeling approach to decompose daily sales of a restaurant into time-dependent multi-factors

MHF2004-3 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Cubic pencils and Painlevé Hamiltonians

MHF2004-4 Atsushi KAWAGUCHI, Koji YONEMOTO & Takashi YANAGAWA
Estimating the correlation dimension from a chaotic system with dynamic noise

MHF2004-5 Atsushi KAWAGUCHI, Kentarou KITAMURA, Koji YONEMOTO, Takashi YANAGAWA & Kiyofumi YUMOTO
Detection of auroral breakups using the correlation dimension

MHF2004-6 Ryo IKOTA, Masayasu MIMURA & Tatsuyuki NAKAKI
A methodology for numerical simulations to a singular limit

MHF2004-7 Ryo IKOTA & Eiji YANAGIDA
Stability of stationary interfaces of binary-tree type

MHF2004-8 Yuko ARAKI, Sadanori KONISHI & Seiya IMOTO
Functional discriminant analysis for gene expression data via radial basis expansion

MHF2004-9 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Hypergeometric solutions to the q - Painlevé equations

MHF2004-10 Raimundas VIDŪNAS
Expressions for values of the gamma function

MHF2004-11 Raimundas VIDŪNAS
Transformations of Gauss hypergeometric functions

MHF2004-12 Koji NAKAGAWA & Masakazu SUZUKI
Mathematical knowledge browser

MHF2004-13 Ken-ichi MARUNO, Wen-Xiu MA & Masayuki OIKAWA
Generalized Casorati determinant and Positon-Negaton-Type solutions of the Toda lattice equation

MHF2004-14 Nalini JOSHI, Kenji KAJIWARA & Marta MAZZOCCO
Generating function associated with the determinant formula for the solutions of the Painlevé II equation

MHF2004-15 Kouji HASHIMOTO, Ryohei ABE, Mitsuhiro T. NAKAO & Yoshitaka WATANABE
Numerical verification methods of solutions for nonlinear singularly perturbed problem

MHF2004-16 Ken-ichi MARUNO & Gino BIONDINI
Resonance and web structure in discrete soliton systems: the two-dimensional Toda lattice and its fully discrete and ultra-discrete versions

MHF2004-17 Ryuei NISHII & Shinto EGUCHI
Supervised image classification in Markov random field models with Jeffreys divergence

MHF2004-18 Kouji HASHIMOTO, Kenta KOBAYASHI & Mitsuhiro T. NAKAO
Numerical verification methods of solutions for the free boundary problem

MHF2004-19 Hiroki MASUDA
Ergodicity and exponential β-mixing bounds for a strong solution of Lévy-driven stochastic differential equations

MHF2004-20 Setsuo TANIGUCHI
The Brownian sheet and the reflectionless potentials

MHF2004-21 Ryuei NISHII & Shinto EGUCHI
Supervised image classification based on AdaBoost with contextual weak classifiers

MHF2004-22 Hideki KOSAKI
On intersections of domains of unbounded positive operators

MHF2004-23 Masahisa TABATA & Shoichi FUJIMA
Robustness of a characteristic finite element scheme of second order in time increment

MHF2004-24 Ken-ichi MARUNO, Adrian ANKIEWICZ & Nail AKHMEDIEV
Dissipative solitons of the discrete complex cubic-quintic Ginzburg-Landau equation

MHF2004-25 Raimundas VIDŪNAS
Degenerate Gauss hypergeometric functions

MHF2004-26 Ryo IKOTA
The boundedness of propagation speeds of disturbances for reaction-diffusion systems

MHF2004-27 Ryusuke KON
Convex dominates concave: an exclusion principle in discrete-time Kolmogorov systems

MHF2004-28 Ryusuke KON
Multiple attractors in host-parasitoid interactions: coexistence and extinction

MHF2004-29 Kentaro IHARA, Masanobu KANEKO & Don ZAGIER
Derivation and double shuffle relations for multiple zeta values

MHF2004-30 Shuichi INOKUCHI & Yoshihiro MIZOGUCHI
Generalized partitioned quantum cellular automata and quantization of classical CA

MHF2005-1 Hideki KOSAKI
Matrix trace inequalities related to uncertainty principle

MHF2005-2 Masahisa TABATA
Discrepancy between theory and real computation on the stability of some finite element schemes

MHF2005-3 Yuko ARAKI & Sadanori KONISHI
Functional regression modeling via regularized basis expansions and model selection

MHF2005-4 Yuko ARAKI & Sadanori KONISHI
Functional discriminant analysis via regularized basis expansions

MHF2005-5 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Point configurations, Cremona transformations and the elliptic difference Painlevé equations

MHF2005-6 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Construction of hypergeometric solutions to the q - Painlevé equations

MHF2005-7 Hiroki MASUDA
Simple estimators for non-linear Markovian trend from sampled data:
I. ergodic cases

MHF2005-8 Hiroki MASUDA & Nakahiro YOSHIDA
Edgeworth expansion for a class of Ornstein-Uhlenbeck-based models

MHF2005-9 Masayuki UCHIDA
Approximate martingale estimating functions under small perturbations of dynamical systems

MHF2005-10 Ryo MATSUZAKI & Masayuki UCHIDA
One-step estimators for diffusion processes with small dispersion parameters from discrete observations

MHF2005-11 Junichi MATSUKUBO, Ryo MATSUZAKI & Masayuki UCHIDA
Estimation for a discretely observed small diffusion process with a linear drift

MHF2005-27 Shuichi INOKUCHI, Kazumasa HONDA, Hyen Yeal LEE, Tatsuro SATO, Yoshihiro MIZOGUCHI & Yasuo KAWAHARA
On reversible cellular automata with finite cell array

MHF2005-28 Toru KOMATSU
Cyclic cubic field with explicit Artin symbols

MHF2005-29 Mitsuhiro T. NAKAO, Kouji HASHIMOTO & Kaori NAGATOU
A computational approach to constructive a priori and a posteriori error estimates for finite element approximations of bi-harmonic problems

MHF2005-30 Kaori NAGATOU, Kouji HASHIMOTO & Mitsuhiro T. NAKAO
Numerical verification of stationary solutions for Navier-Stokes problems

MHF2005-31 Hidefumi KAWASAKI
A duality theorem for a three-phase partition problem

MHF2005-32 Hidefumi KAWASAKI
A duality theorem based on triangles separating three convex sets

MHF2005-33 Takeaki FUCHIKAMI & Hidefumi KAWASAKI
An explicit formula of the Shapley value for a cooperative game induced from the conjugate point

MHF2005-34 Hideki MURAKAWA
A regularization of a reaction-diffusion system approximation to the two-phase Stefan problem

MHF2006-1 Masahisa TABATA
Numerical simulation of Rayleigh-Taylor problems by an energy-stable finite element scheme

MHF2006-2 Ken-ichi MARUNO & G R W QUISPEL
Construction of integrals of higher-order mappings

MHF2006-3 Setsuo TANIGUCHI
On the Jacobi field approach to stochastic oscillatory integrals with quadratic phase function

MHF2006-4 Kouji HASHIMOTO, Kaori NAGATOU & Mitsuhiro T. NAKAO
A computational approach to constructive a priori error estimate for finite element approximations of bi-harmonic problems in nonconvex polygonal domains

MHF2006-5 Hidefumi KAWASAKI
A duality theory based on triangular cylinders separating three convex sets in R^n

MHF2006-6 Raimundas VIDŪNAS
Uniform convergence of hypergeometric series

MHF2006-7 Yuji KODAMA & Ken-ichi MARUNO
N-Soliton solutions to the DKP equation and Weyl group actions

MHF2006-8 Toru KOMATSU
Potentially generic polynomial

MHF2006-9 Toru KOMATSU
Generic sextic polynomial related to the subfield problem of a cubic polynomial