Potentially generic polynomial

Komatsu, Toru
Faculty of Mathematics, Kyushu University

出版情報：MHF Preprint Series. 2006-8, 2006-03-09. 九州大学大学院数理学研究院
バージョン：
権利関係：

MHF Preprint Series

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

Potentially generic polynomial

T. Komatsu

MHF 2006-8

(Received March 9, 2006)

Faculty of Mathematics
Kyushu University
Fukuoka, JAPAN

Potentially generic polynomial

Toru KOMATSU

§ 1. Introduction

Recently many mathematicians constructed generic polynomials (Hashimoto-Miyake [**4**], Hoshi [**6**], Ledet [**13**], Nakano [**15**], Rikuna [**17**], Smith [**22**],...). In some cases the genericities of the polynomials are guaranteed by some useful sufficient conditions (e.g., Kemper [**8**], Kemper-Mattig [**9**] and see also Jensen-Ledet-Yui [**7**]). In this paper we obtain a necessary condition so that a regular polynomial is generic. A regular polynomial f is potentially generic over a field k if f is generic over a finite extension of k. We present a criterion whether a regular cyclic polynomial is potentially generic or not. This shows that some numerical regular polynomials are not generic. We also study the arithmetic of some numerical regular polynomials due to certain invariants $d(t)$, $\lambda(t)$ and $\mu(t)$.

We first recall some notions on the generic polynomial (cf. Jensen-Ledet-Yui [**7**]) and introduce a new concept a potentially generic 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 for G over k 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 $L = \mathrm{Spl}_K F(\mathfrak{a}, X)$. We say that a k-regular G-polynomial $F(\mathfrak{t}, X) \in k(\mathfrak{t})[X]$ is potentially generic over k when $F(\mathfrak{t}, X)$ is generic over a finite extension of k. In this paper we show a necessary condition to hold that a k-regular $\mathcal{C}_n$-polynomial is potentially generic.

Let n be a positive integer with $\mathrm{char}(k) \nmid n$. Let $F(\mathfrak{t}, X)$ be an irreducible, monic and k-regular $\mathcal{C}_n$-polynomial and put $L = \mathrm{Spl}_{k(\mathfrak{t})} F(\mathfrak{t}, X)$. We fix a generator σ of $\mathrm{Gal}(L/k(\mathfrak{t})) \simeq \mathcal{C}_n$ and a solution $x \in L$ of the equation $F(\mathfrak{t}, X) = 0$. Then it satisfies that $F(\mathfrak{t}, X) = \prod_{i=0}^{n-1}(X - \sigma^i(x))$ and $L = k(\mathfrak{t}, x)$. Let ζ be a primitive n-th root of unity in k^{sep}. For a rational integer $j \in \mathbb{Z}$ we define an element $y_j \in L(\zeta)$ by

$$y_j = \frac{1}{n} \sum_{i=0}^{n-1} \zeta^{-ij} \sigma^i(x),$$

which is called the j-th Lagrange resolvent of x for $L/k(\mathfrak{t})$ (cf. [**2**] § 5.3). Here the element y_j depends on the choice of the elements σ and x. Let $Y_j(\mathfrak{t}, X)$ be a polynomial over $k(\mathfrak{t}, \zeta)$ such that $Y_j(\mathfrak{t}, x) = y_j$. We denote by $g_j(\mathfrak{t}) \in k(\mathfrak{t}, \zeta)$ the product of $(-1)^{j(n-1)}$ and the resultant of the two polynomials $F(\mathfrak{t}, X)$ and $Y_j(\mathfrak{t}, X)$ on the indeterminate X, that is,

$$g_j(\mathfrak{t}) = (-1)^{j(n-1)} \mathrm{Res}_X(F(\mathfrak{t}, X), Y_j(\mathfrak{t}, X)).$$

Proposition 1.1 (Corollary 2.2)**.** *We have* $L(\zeta) = \mathrm{Spl}_{k(\mathfrak{t}, \zeta)}(Y^n - g_j(\mathfrak{t}))$ *provided* $\gcd(j, n) = 1$ *and* $y_j \neq 0$.

Note that $F(\mathfrak{t}, X)$ is potentially generic over k if and only if so is $Y^n - g_j(\mathfrak{t})$ over $k(\zeta)$ when $\gcd(j, n) = 1$ and $y_j \neq 0$. By using the $g_j(\mathfrak{t})$ we also study the arithmetic of the field which is obtained as a specialization of $F(\mathfrak{t}, X)$ (see the sections 3 to 5 below). We next consider a condition so that a polynomial $Y^n - g(t)$ is generic over $k(\zeta)$ where $g(t) \in k(t, \zeta)$ is a non-constant rational function over $k(\zeta)$ with one variable t. For an element $\alpha \in \overline{k}$ we denote by $\mathrm{ram}_n(\alpha, g(t))$ the ramification index of the prime divisor $(t - \alpha)$ in the extension $\mathrm{Spl}_{\overline{k}(t, \zeta)}(Y^n - g(t))$ over $\overline{k}(t, \zeta)$.

Theorem 1.2 (Proposition 2.6)**.** *If $Y^n - g(t)$ is potentially generic for $\mathcal{C}_n$ over $k(\zeta)$, then there exist at most two elements $\alpha \in \overline{k}$ satisfying* $\mathrm{ram}_n(\alpha, g(t)) \geq 3$.

In § 2 we study a necessary condition for the genericity of a regular polynomial and prove Proposition 1.1 and Theorem 1.2. In § 3 we calculate the generators of Kummer extensions for some numerical polynomials. In § 4 and § 5 we show that several regular polynomials are not generic by using Proposition 1.1 and Theorem 1.2. We also study the arithmetic of the extensions obtained as the specializations of the polynomials.

Acknowledgement. The author is grateful to Professor Masanari Kida for the information on the results of Spearman-Williams [**23**] and [**24**]. He is supported by the 21st Century COE Program "Development of Dynamic Mathematics with High Functionality".

§ 2. Necessary condition for the genericity

Let k be a field and n a positive integer with $\mathrm{char}(k) \nmid n$. For an irreducible, monic and k-regular $\mathcal{C}_n$-polynomial $F(\mathfrak{t}, X) \in k(\mathfrak{t})[X]$ let L be the extension field $\mathrm{Spl}_{k(\mathfrak{t})}F(\mathfrak{t}, X)$ and σ a generator of $\mathrm{Gal}(L/k(\mathfrak{t})) \simeq \mathcal{C}_n$. We fix a solution $x \in L$ of $F(\mathfrak{t}, X) = 0$. Then it holds that $L = k(\mathfrak{t}, x)$ and $F(\mathfrak{t}, X) = \prod_{i=0}^{n-1}(X - \sigma^i(x))$. Note that $F(\mathfrak{t}, X)$ is potentially generic over k if and only if so is over $k(\zeta)$ where ζ is a primitive n-th root of unity in k^{sep}. Since $L/k(\mathfrak{t})$ is k-regular, $L(\zeta)/k(\mathfrak{t}, \zeta)$ is a $k(\zeta)$-regular $\mathcal{C}_n$-extension. Kummer theory implies that there exists an element $y \in L(\zeta)$ so that $L(\zeta) = k(\mathfrak{t}, \zeta, y)$ and $y^n \in k(\mathfrak{t}, \zeta)$. One can make such a $y \in L(\zeta)$ by using the elements $x \in L$ and $\sigma \in \mathrm{Gal}(L/k(\mathfrak{t}))$ as follows (cf. [**2**] § 5.3). For a rational integer $j \in \mathbb{Z}$ we define

$$y_j = \frac{1}{n}\sum_{i=0}^{n-1} \zeta^{-ij}\sigma^i(x),$$

which is called the j-th Lagrange resolvent of x for $L/k(\mathfrak{t})$. Here the element y_j depends on the choice of the elements σ and x. Note that $L \cap k(\mathfrak{t}, \zeta) = k(\mathfrak{t})$ since L is k-regular. There exists an extension $\widetilde{\sigma} \in \mathrm{Gal}(L(\zeta)/k(\mathfrak{t}))$ of the action $\sigma \in \mathrm{Gal}(L/k(\mathfrak{t}))$ such that $\widetilde{\sigma}(\zeta) = \zeta$ and $\widetilde{\sigma}(x) = \sigma(x)$.

Lemma 2.1. *We have $\widetilde{\sigma}(y_j) = \zeta^j y_j$ and $y_j^n \in k(\mathfrak{t}, \zeta)$.*

Proof. It follows from the definition that

$$\widetilde{\sigma}(y_j) = \frac{1}{n}\sum_{i=0}^{n-1} \zeta^{-ij}\sigma^{i+1}(x) = \frac{1}{n}\sum_{i=0}^{n-1} \zeta^{-(i-1)j}\sigma^{i}(x) = \zeta^j y_j.$$

Thus we have $y_j^n \in L(\zeta)^{\langle\widetilde{\sigma}\rangle} = k(\mathfrak{t}, \zeta)$. □

Let us denote the rational function $y_j^n \in k(\mathfrak{t}, \zeta)$ by $g_j(\mathfrak{t})$. The definition of $g_j(\mathfrak{t})$ is different from that in the Introduction. Lemma 2.4 below will make sure that the two definitions are equivalent to each other.

Corollary 2.2. *If* $\gcd(j, n) = 1$ *and* $y_j \neq 0$, *then* $L(\zeta) = \mathrm{Spl}_{k(\mathfrak{t},\zeta)}(Y^n - g_j(\mathfrak{t}))$.

Proof. It follows from $\gcd(j, n) = 1$ and $y_j \neq 0$ that $[k(\mathfrak{t}, \zeta, y_j) : k(\mathfrak{t}, \zeta)] = n$. Since $y_j \in L(\zeta)$ and $[L(\zeta) : k(\mathfrak{t}, \zeta)] = n$, we have $L(\zeta) = k(\mathfrak{t}, \zeta, y_j) = \mathrm{Spl}_{k(\mathfrak{t},\zeta)}(Y^n - g_j(\mathfrak{t}))$. □

Remark 2.3. When $\zeta \notin k$ and n is a prime number, one has that $y_1 = n^{-1}\sum_{i=1}^{n-1} \zeta^{-i}(\sigma^i(x) - x) \neq 0$.

The following lemma is useful to calculate the element $g_j(\mathfrak{t}) \in k(\mathfrak{t}, \zeta)$. Let $Y_j(\mathfrak{t}, X)$ be a polynomial in $k(\mathfrak{t}, \zeta)[X]$ such that $Y_j(\mathfrak{t}, x) = y_j$. We define the resultant $\mathrm{Res}_X(p_1(X), p_2(X))$ of two polynomials $p_1(X) = a\prod_{i=1}^{l}(X - \alpha_i)$ and $p_2(X) = b\prod_{j=1}^{m}(X - \beta_j)$ by

$$\mathrm{Res}_X(p_1(X), p_2(X)) = a^m \prod_{i=1}^{l} p_2(\alpha_i) = (-1)^{lm} b^l \prod_{j=1}^{m} p_1(\beta_j).$$

Lemma 2.4. *We have*

$$g_j(\mathfrak{t}) = (-1)^{j(n-1)}\mathrm{Res}_X(F(\mathfrak{t}, X), Y_j(\mathfrak{t}, X)).$$

Proof. It follows from the definition that

$$N_{L(\zeta)/k(\mathfrak{t},\zeta)}(y_j) = \prod_{i=0}^{n-1} Y_j(\mathfrak{t}, \widetilde{\sigma}^i(x)) = \mathrm{Res}_X(F(\mathfrak{t}, X), Y_j(\mathfrak{t}, X)).$$

On the other hand, Lemma 2.1 implies that

$$N_{L(\zeta)/k(\mathfrak{t},\zeta)}(y_j) = \prod_{i=0}^{n-1} \widetilde{\sigma}^i(y_j) = \prod_{i=0}^{n-1} \zeta^{ji} y_j = (-1)^{j(n-1)} y_j^n = (-1)^{j(n-1)} g_j(\mathfrak{t}).$$

Thus the equation of the assertion holds. □

Corollary 2.2 and Lemma 2.4 verify Proposition 1.1.

Remark 2.5. There are several formulas for the resultant, e.g., the determinant of Sylvester's matrix (cf. [**1**] § 3.3).

Let $g(t) \in k(t,\zeta)$ be a non-constant rational function over $k(\zeta)$ with one variable t. We give a necessary condition so that $Y^n - g(t)$ is generic over $k(\zeta)$. As defined in the Introduction we denote by $\mathrm{ram}_n(\alpha, g(t))$ the ramification index of the prime divisor $(t-\alpha)$ in the extension $\mathrm{Spl}_{\overline{k}(t,\zeta)}(Y^n - g(t))/\overline{k}(t,\zeta)$ for an element $\alpha \in \overline{k}$.

Proposition 2.6 (Theorem 1.2)**.** *If the set* $\{\alpha \in \overline{k} | \mathrm{ram}_n(\alpha, g(t)) \geq 3\}$ *has at least three elements, then the polynomial* $Y^n - g(t) \in k(t,\zeta)[Y]$ *is not potentially generic for* $\mathcal{C}_n$ *over* $k(\zeta)$.

For the proof of Proposition 2.6 we use the abc theorem for the function field, which is a corollary of Riemann-Hurwitz formula. For a non-constant rational function $u = u(t) \in \overline{k}(t)$ let us consider a map $u : \mathbb{P}^1(\overline{k}) \to \mathbb{P}^1(\overline{k})$, $a \mapsto u(a)$. For an element $b \in \mathbb{P}^1(\overline{k}) - \{0, \infty\}$ we denote by $Z(b,u)$ the union set $u^{-1}(\{0, b, \infty\})$ of the inverse images of three points $0, b$ and ∞ by the map u.

Lemma 2.7. *If the extension* $\overline{k}(t)/\overline{k}(u)$ *is separable, then* $[\overline{k}(t) : \overline{k}(u)] \leq \sharp Z(b,u) - 2$.

Proof. Riemann-Hurwitz formula implies that

$$\begin{aligned} -2 &\geq -2d_u + \textstyle\sum_{a \in \mathbb{P}^1(\overline{k})} (e_u(a) - 1) \\ &\geq -2d_u + \textstyle\sum_{a \in Z(b,u)} (e_u(a) - 1) \\ &= -2d_u + 3d_u - \sharp Z(b,u) \\ &= d_u - \sharp Z(b,u) \end{aligned}$$

where $d_u = [\overline{k}(t) : \overline{k}(u)]$ and $e_u(a)$ is the ramification index of u at $a \in \mathbb{P}^1(\overline{k})$. Thus we have $d_u \leq \sharp Z(b,u) - 2$. □

Proof of Proposition 2.6. Now suppose $Y^n - g(t)$ is potentially generic over $k(\zeta)$, then $Y^n - g(t)$ is generic over $\overline{k}$. One may assume that $g(t)$ is a monic polynomial over $\overline{k}$ of the form $g(t) = \prod_{i=1}^{l} (t - \alpha_i)^{m_i}$ where $\alpha_i \in \overline{k}$ and $m_i = \mathrm{ord}_{\alpha_i} g(t)$ are positive integers. Let s be an indeterminate and $K = \overline{k}(s)$. Due to the genericity of $Y^n - g(t)$ there exists a rational function $h(s) \in K$ such that $\mathrm{Spl}_K(Z^n - s) =$

$\mathrm{Spl}_K(Y^n - g(h(s)))$, that is, the Kummer extension $\mathrm{Spl}_K(Z^n - s)$ should be obtained as a suitable specialization $t = h(s) \in K$. It follows from Kummer theory that $g(h(s))/s^j \in K^n$ for an integer $j \in \mathbb{Z}$. Let $h_1(s)$ and $h_2(s)$ be polynomials in $\overline{k}[s]$ with no common zeros such that $h(s) = h_1(s)/h_2(s)$. Then we have $h_2(s)^{-m}s^{-j}\prod_{i=1}^{l}(h_1(s) - \alpha_i h_2(s))^{m_i} \in K^n$ where m is equal to the degree $\deg_t g(t) = \sum_{i=1}^{l} m_i$ of the polynomial $g(t)$. Since α_i are distinct, the polynomials $h_1(s) - \alpha_i h_2(s)$ and $h_2(s)$ are relatively prime to each other. Thus there exist polynomials $p_i(s) \in \overline{k}[s]$ and non-negative integers $j_i \in \mathbb{Z}$ such that $h_1(s) - \alpha_i h_2(s) = s^{j_i}p_i(s)^{r_i}$ and $p_i(0) \neq 0$ where $r_i = \mathrm{ram}_n(\alpha_i, g(t))$. Note that $j_i = \mathrm{ord}_0(h_1(s) - \alpha_i h_2(s))$. Thus one may assume $j_2 = j_3 = 0$. Here it holds that $(\alpha_2 - \alpha_3)s^{j_1}p_1(s)^{r_1} + (\alpha_3 - \alpha_1)p_2(s)^{r_2} + (\alpha_1 - \alpha_2)p_3(s)^{r_3} = 0$. Let u_1 and u_2 be rational functions in K such that

$$u_1 = \frac{(\alpha_2 - \alpha_3)s^{j_1}p_1(s)^{r_1}}{(\alpha_1 - \alpha_2)p_3(s)^{r_3}}, \quad u_2 = \frac{(\alpha_3 - \alpha_1)p_2(s)^{r_2}}{(\alpha_1 - \alpha_2)p_3(s)^{r_3}}.$$

Then one has $u_1 + u_2 + 1 = 0$, which means that $\overline{k}(u_1) = \overline{k}(u_2)$. Let M be the maximal separable extension of $\overline{k}(u_i)$ contained in K, and q be the degree of the purely inseparable extension K/M. Then there exist rational functions $\widetilde{u_i}(s) \in K$ such that $\widetilde{u_i}(s^q) = u_i(s)$ for $i = 1$ and 2. Since $p_1(s)$, $p_2(s)$ and $p_3(s)$ are relatively prime to each other, we have $\widetilde{p_i}(s^q) = p_i(s)$ for some polynomials $\widetilde{p_i}(s) \in \overline{k}[s]$, respectively. In fact, r_i are prime to q since r_i are divisors of n. Then $K/\overline{k}(\widetilde{u_1})$ is a separable extension. Let us denote by d_i the degrees $\deg_s \widetilde{p_i}(s)$ of the polynomials $\widetilde{p_i}(s) \in \overline{k}[s]$, respectively. It follows from $\widetilde{u_1} + 1 = -\widetilde{u_2}$ that $\sharp Z(-1, \widetilde{u_1}) \leq 1 + \sum_{i=1}^{3} d_i$. Here one has that $[K : \overline{k}(\widetilde{u_i})] = \max\{r_1 d_1 + j_1/q, r_2 d_2, r_3 d_3\} \geq (r_1 d_1 + r_2 d_2 + r_3 d_3)/3$. Lemma 2.7 implies

$$r_1 d_1 + r_2 d_2 + r_3 d_3 \leq 3[K : \overline{k}(\widetilde{u_1})] \leq 3(d_1 + d_2 + d_3 - 1).$$

This means that $3 + \sum_{i=1}^{3}(r_i - 3)d_i \leq 0$, which is impossible provided $r_i \geq 3$ for $i = 1, 2$ and 3. Hence we conclude that the set $\{\alpha \in \overline{k} | \mathrm{ram}_n(\alpha, g(t)) \geq 3\}$ has at most two elements. $\square$

The number $\mathrm{ram}_n(\alpha, g(t))$ is equal to the minimal positive integer r such that $r\mathrm{ord}_\alpha g(t) \in n\mathbb{Z}$ where $\mathrm{ord}_\alpha g(t)$ is the order at α of $g(t)$. We define a positive integer

$\mathrm{ram}_n(\infty, g(t))$ to be the minimal positive divisor r of n satisfying $r\mathrm{ord}_\infty g(t) \in n\mathbb{Z}$ as for the case $\alpha \in \overline{k}$.

Corollary 2.8. *If the set* $\{\alpha \in \overline{k} \cup \{\infty\} | \mathrm{ram}_n(\alpha, g(t)) \geq 3\}$ *has at least three elements, then the polynomial* $Y^n - g(t)$ *is not potentially generic for* $\mathcal{C}_n$ *over* $k(\zeta)$.

Proof. Let α_1, α_2 and $\alpha_3 \in \overline{k} \cup \{\infty\}$ be distinct three elements which satisfy $\mathrm{ram}_n(\alpha, g(t)) \geq 3$. It follows from Proposition 2.6 that one may assume $\alpha_3 = \infty$. For an element $a \in \overline{k}$ with $a \notin \{\alpha_1, \alpha_2, \alpha_3\}$ we put $g_a(t) = g(1/t + a) \in k(t, \zeta, a)$. Then the set $\{\alpha \in \overline{k} | \mathrm{ram}_n(\alpha, g_a(t)) \geq 3\}$ has distinct three elements $1/(\alpha_i - a) \in \overline{k}$ for $i = 1, 2$ and 3. Proposition 2.6 implies that $Y^n - g_a(t)$ is not potentially generic over $k(\zeta, a)$. Here the potential genericity of $Y^n - g(t)$ over $k(\zeta)$ is equivalent to that of $Y^n - g_a(t)$ over $k(\zeta, a)$. Thus $Y^n - g(t)$ is not potentially generic over $k(\zeta)$. □

For an irreducible, monic and k-regular $\mathcal{C}_n$-polynomial $F(t, X) \in k(t)[X]$ we denote by $e_3(F)$ the sum of the degrees of the prime divisors of $k(t)$ whose ramification indices in the extension $\mathrm{Spl}_{k(t)} F(t, X)/k(t)$ are greater than 2.

Corollary 2.9. *If* $e_3(F) \geq 3$, *then* $F(t, X)$ *is not potentially generic for* $\mathcal{C}_n$ *over* k.

Proof. Since $F(t, X)$ is regular over k, one sees that the number $e_3(F)$ is equal to $\sharp\{\alpha \in \overline{k} \cup \{\infty\} | \mathrm{ram}_n(\alpha, g_F(t)) \geq 3\}$ where $g_F(t)$ is the rational function described in this section so that $\mathrm{Spl}_{k(t,\zeta)} F(t, X) = \mathrm{Spl}_{k(t,\zeta)}(Y^n - g_F(t))$. □

§ 3. Some numerical examples of general degree cases

Let $n \in \mathbb{Z}$ be a rational integer greater than 2 and ζ a primitive n-th root of unity in $\overline{\mathbb{Q}}$ and $\omega = \zeta + \zeta^{-1}$. Rikuna [**16**] defined a polynomial

$$R_n(t, X) = \frac{\zeta^{-1}(X - \zeta)^n - \zeta(X - \zeta^{-1})^n}{\zeta^{-1} - \zeta} - t\frac{(X - \zeta)^n - (X - \zeta^{-1})^n}{\zeta^{-1} - \zeta},$$

which is a regular $\mathcal{C}_n$-polynomial over $k = \mathbb{Q}(\omega)$. It is already shown that $R_n(t, X)$ is generic over k if n is odd (Rikuna [**16**]) and that $R_n(t, X)$ is generic not over k but over $k(\zeta)$ when n is even (Komatsu [**11**]). Thus the polynomials $R_n(t, X)$ with even n are examples of the non-generic but potentially generic polynomials. Let L

be the field $\mathrm{Spl}_{k(t)}R_n(t,X)$ and x a solution in L of $R_n(t,X)=0$. Then one sees that $L=k(t,x)$ and $\mathrm{Gal}(L/k(t))=\langle\sigma\rangle\simeq\mathcal{C}_n$ where

$$\sigma^i(x)=\frac{(\zeta^{i-1}-\zeta)x-(\zeta^i-1)}{(\zeta^i-1)x-(\zeta^{i+1}-\zeta^{-1})}$$

(cf. Rikuna [**16**], Komatsu [**11**]). Let y_j be the j-th Lagrange resolvent of x for $L/k(t)$, that is, $y_j=n^{-1}\sum_{i=0}^{n-1}\zeta^{-ij}\sigma^i(x)$.

Proposition 3.1. *For a rational integer $j\in\mathbb{Z}$ with $1\le j\le n-1$ we have $y_j^n=(t-\zeta)^j(t-\zeta^{-1})^{n-j}$ and $y_0=t$.*

We use the following lemma.

Lemma 3.2. *For a rational integer $j\in\mathbb{Z}$ with $0\le j\le n-1$ we have*

$$\frac{1}{n}\sum_{i=0}^{n-1}\zeta^{-ij}\frac{\zeta^{i-1}Z-\zeta}{\zeta^iZ-1}=\begin{cases}\dfrac{\zeta^{-1}Z^n-\zeta}{Z^n-1} & \text{if } j=0,\\ \dfrac{(\zeta^{-1}-\zeta)Z^j}{Z^n-1} & \text{otherwise.}\end{cases}$$

Proof. It follows from the definition that

$$\begin{aligned}&\frac{1}{n}\sum_{i=0}^{n-1}\zeta^{-ij}\frac{\zeta^{i-1}Z-\zeta}{\zeta^iZ-1}\\ &=\frac{1}{n}\sum_{i=0}^{n-1}\zeta^{-ij}\frac{\zeta^{i-1}Z-\zeta}{Z^n-1}\sum_{m=0}^{n-1}(\zeta^iZ)^m\\ &=\frac{1}{n(Z^n-1)}\left(\zeta^{-1}\sum_{m=0}^{n-1}\sum_{i=0}^{n-1}\zeta^{i(m+1-j)}Z^{m+1}-\zeta\sum_{m=0}^{n-1}\sum_{i=0}^{n-1}\zeta^{i(m-j)}Z^m\right).\end{aligned}$$

Note that $\sum_{i=0}^{n-1}\zeta^{im}$ is equal to n if $m\equiv 0 \pmod n$ and 0 otherwise. Thus we have the equation of the assertion. □

Proof of Proposition 3.1. By substituting $Z=(x-\zeta)/(x-\zeta^{-1})$ in the equation of Lemma 3.2 we have $y_0=(\zeta^{-1}(x-\zeta)^n-\zeta(x-\zeta^{-1})^n)/((x-\zeta)^n-(x-\zeta^{-1})^n)=t$. Here one has

$$t-\zeta^{\pm1}=\frac{(\zeta^{-1}-\zeta)(x-\zeta^{\pm1})^n}{(x-\zeta)^n-(x-\zeta^{-1})^n},$$

respectively. When $1\le j\le n-1$, Lemma 3.2 with $Z=(x-\zeta)/(x-\zeta^{-1})$ implies that

$$y_j^n=\frac{(\zeta^{-1}-\zeta)^n(x-\zeta)^{jn}(x-\zeta^{-1})^{(n-j)n}}{((x-\zeta)^n-(x-\zeta^{-1})^n)^n}=(t-\zeta)^j(t-\zeta^{-1})^{n-j}.\quad\square$$

Corollary 3.3. *We have $L(\zeta)=\mathrm{Spl}_{k(t,\zeta)}(Y^n-(t-\zeta)/(t-\zeta^{-1}))$. In particular, $R_n(t,X)$ is generic over $k(\zeta)$ and potentially generic over k.*

Proof. Corollary 2.2 and Proposition 3.1 imply that

$$L(\zeta) = \mathrm{Spl}_{k(t,\zeta)}(Y^n - (t-\zeta)(t-\zeta^{-1})^{n-1}) = \mathrm{Spl}_{k(t,\zeta)}(Y^n - (t-\zeta)/(t-\zeta^{-1})).$$

Since $(t-\zeta)/(t-\zeta^{-1})$ is linear fractional, it follows from Kummer theory that $Y^n - (t-\zeta)/(t-\zeta^{-1})$ is generic over $k(\zeta)$ and so is $R_n(t,X)$. □

Let $k = \mathbb{Q}(\omega)$ be as in the case of $R_n(t,X)$. For an even integer n greater than 2, Hashimoto and Rikuna [**5**] defined a polynomial $HR_n(\mathfrak{t},X) \in k(\mathfrak{t})[X]$ with two parameters $\mathfrak{t} = (t_1,t_2)$ such that

$$\begin{aligned} HR_n(\mathfrak{t},X) = X^n + &\textstyle\sum_{i=1}^{(n-2)/2} B(n,i)(T_1t_2)^i X^{n-2i} \\ &-(\omega^2-4)T_1^{(n-2)/2}t_2^{n/2} \in k(t_1,t_2)[X] \end{aligned}$$

where $T_1 = t_1^2 - \omega t_1 + 1$ and $B(n,i) = \binom{n-i-1}{i-1} + \binom{n-i}{i}$. Here $\binom{m_1}{m_2}$ denotes the binomial coefficient $m_1!/(m_2!(m_1-m_2)!)$.

Proposition 3.4 (Hashimoto-Rikuna [**5**]). *The polynomial $HR_n(\mathfrak{t},X)$ is k-generic for $\mathcal{C}_n$.*

We calculate the rational function $g_j(\mathfrak{t})$ for $HR_n(\mathfrak{t},X)$.

Lemma 3.5. *We have*

$$\mathrm{Spl}_{k(\mathfrak{t},\zeta)} HR_n(\mathfrak{t},X) = \mathrm{Spl}_{k(\mathfrak{t},\zeta)}(Y^n - (T_1t_2)^{n/2}\frac{t_1-\zeta}{t_1-\zeta^{-1}}).$$

Proof. Let us denote $\mathrm{Spl}_{k(\mathfrak{t})} HR_n(\mathfrak{t},X)$ by L. For a solution z_1 of $Z^n - (T_1t_2)^{n/2}(t_1-\zeta)/(t_1-\zeta^{-1}) = 0$ in $\overline{k(\mathfrak{t})}$ we put $z_2 = -T_1t_2/z_1$. The argument in [**5**] implies that

$$HR_n(\mathfrak{t},X) = \prod_{i=0}^{n}(X - (\zeta^i z_1 + \zeta^{-i} z_2)),$$

$L = k(\mathfrak{t}, z_1 + z_2)$ and that the Galois group $\mathrm{Gal}(L/k(\mathfrak{t}))$ is generated by $\sigma \in \mathrm{Gal}(L/k(\mathfrak{t}))$ such that $\sigma^i(z_1+z_2) = \zeta^i z_1 + \zeta^{-i} z_2$. Thus the j-th Lagrange resolvent y_j is equal to

$$y_j = \begin{cases} z_1 & \text{if } j \equiv 1 \pmod{n}, \\ z_2 & \text{if } j \equiv -1 \pmod{n}, \\ 0 & \text{otherwise.} \end{cases}$$

Hence the element $g_1(\mathfrak{t}) = y_1^n$ is equal to $z_1^n = (T_1t_2)^{n/2}(t_1-\zeta)/(t_1-\zeta^{-1})$. □

Corollary 3.6. *Let K be a finite number field containing $k = \mathbb{Q}(\omega)$ and $\mathfrak{p}$ a prime ideal of K with $\mathfrak{p} \nmid n$. For an $\mathfrak{a} = (a_1,a_2) \in K^2$ with $(a_1^2 - \omega a_1 + 1)a_2 \neq 0$, the* *ramification index of* $\mathfrak{p}$ *in the extension* $\mathrm{Spl}_K HR_n(\mathfrak{a}, X)/K$ *is equal to the order of the rational integer*

$$(\frac{n}{2}-1)\max\{\mathrm{ord}_{\mathfrak{p}}(a_1^2-\omega a_1+1),0\}+\frac{n}{2}\mathrm{ord}_{\mathfrak{p}}(a_2)$$

in the additive group $\mathbb{Z}/n\mathbb{Z}$. *Here* $\mathrm{ord}_{\mathfrak{p}}$ *is the* $\mathfrak{p}$*-adic additive valuation of* K *so that* $\mathrm{ord}_{\mathfrak{p}}(K^{\times})=\mathbb{Z}$.

§ 4. Several examples of cubic polynomials

We prepare some lemmas for the calculation of the ramification in the extension over an algebraic number field.

Lemma 4.1 (cf. [**3**]). *Let* l *be a prime number and* $\mathfrak{p}$ *a prime ideal of* $\mathbb{Q}(\zeta_l)$. *Let* $c \in \mathbb{Q}(\zeta_l)$ *and* $z \in \overline{\mathbb{Q}}$ *be algebraic numbers such that* $z^l = c \neq 0$.
(1) *When* $v_{\mathfrak{p}}(c) \not\equiv 0 \pmod{l}$, *the extension* $\mathbb{Q}(\zeta_l, z)/\mathbb{Q}(\zeta_l)$ *is ramified at* $\mathfrak{p}$.
(2) *If* $v_{\mathfrak{p}}(c) \equiv 0 \pmod{l}$ *and* $\mathfrak{p} \nmid l$, *then* $\mathbb{Q}(\zeta_l, z)/\mathbb{Q}(\zeta_l)$ *is unramified at* $\mathfrak{p}$.
(3) *For the case* $v_{\mathfrak{p}}(c) = 0$, *the prime ideal* $\mathfrak{p} = (\zeta_l - 1)$ *of* $\mathbb{Q}(\zeta_l)$ *above* l *ramifies, remains prime and splits completely in* $\mathbb{Q}(\zeta_l, z)/\mathbb{Q}(\zeta_l)$ *if and only if the valuation* $v_{\mathfrak{p}}(c^{l-1}-1)$ *is less than* l, *equal to* l *and greater than* l, *respectively.*

Corollary 4.2. *Let the notation be as in Lemma* 4.1. *We assume that there exists an element* $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ *of order* m *such that* $N_{\langle\tau\rangle}(c) = \prod_{i=0}^{m-1}\tau^i(c) = 1$. *Then the prime ideal* $\mathfrak{p} = (\zeta_l - 1)$ *of* $\mathbb{Q}(\zeta_l)$ *above* l *ramifies, remains prime and splits completely in the extension* $\mathbb{Q}(\zeta_l, z)/\mathbb{Q}(\zeta_l)$ *if and only if the valuation* $v_{\mathfrak{p}}(c^m - 1)$ *is less than* l, *equal to* l *and greater than* l, *respectively.*

Proof. Since $\mathfrak{p} = (\zeta_l - 1)$ is a unique prime ideal of $\mathbb{Q}(\zeta_l)$ above l, we have $\tau(\mathfrak{p}) = \mathfrak{p}$ and $v_{\mathfrak{p}}(c) = v_{\mathfrak{p}}(\tau^i(c))$. This implies that $mv_{\mathfrak{p}}(c) = v_{\mathfrak{p}}(1) = 0$ and $v_{\mathfrak{p}}(c) = 0$. Note that $\tau(c) \equiv c \pmod{\mathfrak{p}}$ for $\mathcal{O}_{\mathbb{Q}(\zeta_l)}/\mathfrak{p} \simeq \mathbb{F}_l$. Thus one has that $c^m \equiv N_{\langle\tau\rangle}(c) \equiv 1 \pmod{\mathfrak{p}}$. Since m is a divisor of $l-1$, we have $c^l - c = c(c^m-1)\sum_{i=0}^{(l-1)/m-1} c^{mi}$. It holds that $\sum_{i=0}^{(l-1)/m-1} c^{mi} \equiv (l-1)/m \not\equiv 0 \pmod{\mathfrak{p}}$. This means that $v_{\mathfrak{p}}(c^m-1) = v_{\mathfrak{p}}(c^l - c)$. Hence Lemma 4.1 (3) shows the assertion. □

Let us consider a cubic polynomial

$$f_0(t, X) = X^3 - tX^2 - (t+3)X - 1$$

over $\mathbb{Q}(t)$, which is called the simplest cubic polynomial of Shanks type [**21**]. The discriminant of the polynomial $f_0(t,X)$ is equal to $(t^2+3t+9)^2$. For the relation $f_0(t,X)=R_3(t/3,X)$ one can think that the Rikuna's polynomial $R_n(t,X)$ at the previous section is a generalization of the $f_0(t,X)$. The field $L_0=\mathrm{Spl}_{\mathbb{Q}(t)}f_0(t,X)$ is a cyclic cubic extension of $\mathbb{Q}(t)$ whose Galois group $\mathrm{Gal}(L_0/\mathbb{Q}(t))$ is generated by an element σ satisfying

$$\sigma(x)=\frac{-x-1}{x}=-x^2+tx+(t+2),\quad \sigma^2(x)=\frac{-1}{x+1}=x^2-(t+1)x-2.$$

The 1st Lagrange resolvent $y=(x+\zeta^{-1}\sigma(x)+\zeta^{-2}\sigma^2(x))/3$ is equal to $Y(t,x)$ where

$$Y(t,X)=((2\zeta+1)X^2-((2\zeta+1)t+(\zeta-1))X-(\zeta+1)t-4\zeta-2)/3\in\mathbb{Q}(t,\zeta)[X]$$

and ζ is a primitive 3rd root of unity in $\overline{\mathbb{Q}}$. Proposition 2.4 implies

$$\begin{aligned} g(t) &= \mathrm{Res}_X(f_0(t,X),Y(t,X)) \\ &= (t^3+(3\zeta+6)t^2+(9\zeta+18)t+(27\zeta+27))/27 \\ &= (t-3\zeta)(t+3\zeta+3)^2/27. \end{aligned}$$

Lemma 4.3. *We have*

$$L_0(\zeta)=\mathrm{Spl}_{\mathbb{Q}(t,\zeta)}(Y^3-\frac{t-3\zeta}{t+3\zeta+3}).$$

Let us denote $(t-3\zeta)(t+3\zeta+3)=t^2+3t+9$ by $d_0(t)$. For a prime number $p\neq 3$ we define $U_{0,p}(\mathbb{Q})=\{a\in\mathbb{Q}|v_p(a)<0 \text{ or } v_p(d_0(a))\equiv 0 \pmod 3\}$. The set $U_{0,3}(\mathbb{Q})$ is defined to be $U_{0,3}(\mathbb{Q})=\{a\in\mathbb{Q}|v_3(a+3/2)\neq 1,2\}$. The following lemma was shown in [**11**], which is also seen in the same way as for the proof of Proposition 4.11 below.

Lemma 4.4 (Komatsu [**11**])**.** *For a rational number $a\in\mathbb{Q}$ the conductor* $\mathrm{cond}(L)$ *of the extension $L=\mathrm{Spl}_{\mathbb{Q}}f_0(a,X)$ is equal to $\prod_p p^{r_p}$ where*

$$r_p=\begin{cases} 1 & \text{if } p\neq 3 \text{ and } a\notin U_{0,p},\\ 2 & \text{if } p=3 \text{ and } a\notin U_{0,3},\\ 0 & \text{otherwise.}\end{cases}$$

Remark 4.5. For a cyclic extension L/K of prime degree l we have a relation $\mathrm{cond}(L/K)^{l-1}=\mathrm{disc}(L/K)$ between the conductor $\mathrm{cond}(L/K)$ and the discriminant $\mathrm{disc}(L/K)$ of L/K (cf. [**19**]).

Remark 4.6. It is well-known that $f_0(t,X)$ is a generic $\mathcal{C}_3$-polynomial over $\mathbb{Q}$ (cf. [**20**]).

In the same way as for $f_0(t,X)$ one can calculate the invariants for cubic polynomials

$$\begin{aligned} f_1(t,X) &= X^3-(t^3-2t^2+3t-3)X^2-t^2X-1,\\ f_2(t,X) &= X^3+3(3t^2-3t+2)X^2+3X-1,\\ f_3(t,X) &= X^3-t(t^2+t+3)(t^2+2)X^2-(t^3+2t^2+3t+3)X-1,\\ f_4(t,X) &= X^3+(t^8+2t^6-3t^5+3t^4-4t^3+5t^2-3t+3)X^2-t^2(t^3-2)X-1. \end{aligned}$$

The $f_1(t,X)$ was given by Lecacheux [**12**] and the latters $f_i(t,X)$ for $i=2,3$ and 4 were obtained by Kishi [**10**]. The discriminants $\mathrm{disc} f_i(t,X)$ of the polynomials are

$$\begin{aligned} \mathrm{disc}_X f_1(t,X) &= (t-1)^2(t^2+3)^2(t^2-3t+3)^2,\\ \mathrm{disc}_X f_2(t,X) &= 3^6(2t-1)^2(t^2-t+1)^2,\\ \mathrm{disc}_X f_3(t,X) &= (t^2+1)^2(t^2+3)^2(t^4+t^3+4t^2+3)^2,\\ \mathrm{disc}_X f_4(t,X) &= (t^2-t+1)^2(t^3+t-1)^2(t^4-t^3+t^2-3t+3)^2\\ &\quad\times(t^4+2t^3+4t^2+3t+3)^2. \end{aligned}$$

For $i=1,2,3$ and 4 let us denote $\mathrm{Spl}_{\mathbb{Q}(t)} f_i(t,X)$ by L_i, respectively.

Proposition 4.7. *We have*

$$\begin{aligned} L_1(\zeta) &= \mathrm{Spl}_{\mathbb{Q}(t,\zeta)}\left(Y^3-\frac{(t-2\zeta-1)(t-\zeta-2)}{(t+2\zeta+1)(t+\zeta-1)}\right),\\ L_2(\zeta) &= \mathrm{Spl}_{\mathbb{Q}(t,\zeta)}\left(Y^3-\frac{t-\zeta-1}{t+\zeta}\right),\\ L_3(\zeta) &= \mathrm{Spl}_{\mathbb{Q}(t,\zeta)}\left(Y^3-\frac{(t-2\zeta-1)(t^2-\zeta t+\zeta+2)}{(t+2\zeta+1)(t^2+(\zeta+1)t-\zeta+1)}\right),\\ L_4(\zeta) &= \mathrm{Spl}_{\mathbb{Q}(t,\zeta)}\left(Y^3-\frac{(t-\zeta-1)(t^2+\zeta t-2\zeta-1)(t^2+t-\zeta+1)}{(t+\zeta)(t^2-(\zeta+1)t+2\zeta+1)(t^2+t+\zeta+2)}\right). \end{aligned}$$

Corollary 4.8 (Kishi [**10**]). *We have* $\mathrm{Spl}_{\mathbb{Q}(t)} f_2(t,X)=\mathrm{Spl}_{\mathbb{Q}(t)} f_0(-3t,X)$.

Proof. Proposition 4.7 implies that $\mathrm{Spl}_{\mathbb{Q}(t,\zeta)} f_2(t,X)=\mathrm{Spl}_{\mathbb{Q}(t,\zeta)} f_0(-3t,X)$. Here two fields $\mathrm{Spl}_{\mathbb{Q}(t,\zeta)} f_2(t,X)$ and $\mathrm{Spl}_{\mathbb{Q}(t,\zeta)} f_0(-3t,X)$ are $\mathcal{C}_3\times\mathcal{C}_2$-extensions of $\mathbb{Q}(t)$. Thus the two fields have unique subextensions M of $\mathbb{Q}(t)$ with $[M:\mathbb{Q}(t)]=3$, which are equal to $\mathrm{Spl}_{\mathbb{Q}(t)} f_2(t,X)$ and $\mathrm{Spl}_{\mathbb{Q}(t)} f_0(-3t,X)$, respectively. Thus we have $\mathrm{Spl}_{\mathbb{Q}(t)} f_2(t,X)=\mathrm{Spl}_{\mathbb{Q}(t)} f_0(-3t,X)$. $\square$

By Propositions 2.6 and 4.7 we have

Corollary 4.9. *The polynomials $f_1(t,X)$, $f_3(t,X)$ and $f_4(t,X)$ are not potentially generic over $\mathbb{Q}$.*

Proof of Proposition 4.7. For $i = 1, 2, 3$ and 4 let x_i be solutions of $f_i(t, X) = 0$ in L_i, respectively. Then one can check that the following elements σ_i generate the Galois groups $\mathrm{Gal}(L_i/\mathbb{Q}(t)) \simeq \mathcal{C}_3$ and can calculate the the cubes $\lambda_i(t) \in \mathbb{Q}(t, \zeta)$ of 1st Lagrange resolvents by using Lemma 2.4, respectively.

$$\begin{aligned}
\sigma_1(x_1) &= -(t^2 - t + 1)/(t - 1)x_1^2 + (t^4 - 2t^3 + 4t^2 - 4t + 2)x_1 \\
&\quad + (t^4 - 2t^3 + 3t^2 - 3t + 2)/(t - 1), \\
\lambda_1(t) &= (t - 2\zeta - 1)(t + 2\zeta + 1)^2(t - \zeta - 2)(t + \zeta - 1)^2(t - \zeta - 1)^3/27, \\
\sigma_2(x_2) &= -(3t^2 - 3t + 1)/(2t - 1)x_2^2 \\
&\quad - (27t^4 - 54t^3 + 54t^2 - 26t + 5)/(2t - 1)x_2 \\
&\quad - (9t^3 - 9t^2 + 6t - 2)/(2t - 1), \\
\lambda_2(t) &= -(t - \zeta - 1)(t + \zeta)^2(3t - \zeta - 2)^3, \\
\sigma_3(x_3) &= -(t^4 + t^3 + 3t^2 + t + 1)/(t^2 + 1)x_3^2 \\
&\quad + t(t^8 + 2t^7 + 9t^6 + 11t^5 + 25t^4 + 18t^3 + 25t^2 + 8t + 7)/(t^2 + 1)x_3 \\
&\quad + (t^7 + 2t^6 + 7t^5 + 8t^4 + 13t^3 + 8t^2 + 6t + 2)/(t^2 + 1), \\
\lambda_3(t) &= (t - 2\zeta - 1)(t + 2\zeta + 1)^2 \\
&\quad \times (t^2 - \zeta t + \zeta + 2)(t^2 + (\zeta + 1)t - \zeta + 1)^2(t^2 - \zeta t + 1)^3/27, \\
\sigma_4(x_4) &= -(t^6 + t^4 - 2t^3 + t^2 - t + 1)/(t^3 + t - 1)x_4^2 \\
&\quad - (t^{14} + 3t^{12} - 5t^{11} + 6t^{10} - 12t^9 + 17t^8 - 18t^7 \\
&\qquad + 24t^6 - 23t^5 + 21t^4 - 17t^3 + 11t^2 - 6t + 2)/(t^3 + t - 1)x_4 \\
&\quad - (t^2 + 1)(t^7 + t^5 - 3t^4 + 2t^3 - t^2 + 3t - 2)/(t^3 + t - 1), \\
\lambda_4(t) &= -(t - \zeta - 1)(t + \zeta)^2(t^2 + \zeta t - 2\zeta - 1)(t^2 - (\zeta + 1)t + 2\zeta + 1)^2 \\
&\quad \times (t^2 + t - \zeta + 1)(t^2 + t + \zeta + 2)^2(t^3 - \zeta t - 1)^3/27.
\end{aligned}$$

Thus the equations of the assertion hold. $\square$

REMARK 4.10. On $f_1(t, X)$ Washington [**26**] gave a generator ρ of $\mathrm{Gal}(L_1/\mathbb{Q}(t))$ satisfying $\rho(x) = -(x + 1)/((t^2 - t + 1)x + t)$. In fact, one has $\rho = \sigma_1^2$.

For $i = 1, 2, 3$ and 4 let $\lambda_i(t) \in \mathbb{Q}(\zeta)[t]$ be the polynomials as in the proof of Proposition 4.7. For $j = 1, 2$ and 3 let $d_{i,j}(t)$ be the products of all the monic prime divisors whose multiplicities in $\lambda_i(t)$ are equal to j, respectively, that is,

$$\begin{aligned}
&d_{1,1}(t) = (t - 2\zeta - 1)(t - \zeta - 2), \quad d_{1,2}(t) = (t + 2\zeta + 1)(t + \zeta - 1), \\
&d_{2,1}(t) = t - \zeta - 1, \qquad\qquad\qquad\quad d_{2,2}(t) = t + \zeta, \\
&d_{3,1}(t) = (t - 2\zeta - 1)(t^2 - \zeta t + \zeta + 2), \\
&d_{3,2}(t) = (t + 2\zeta + 1)(t^2 + (\zeta + 1)t - \zeta + 1), \\
&d_{4,1}(t) = (t - \zeta - 1)(t^2 + \zeta t - 2\zeta - 1)(t^2 + t - \zeta + 1), \\
&d_{4,2}(t) = (t + \zeta)(t^2 - (\zeta + 1)t + 2\zeta + 1)(t^2 + t + \zeta + 2).
\end{aligned}$$

Note that $\tau(d_{i,1}(t)) = d_{i,2}(t)$ for $\tau \in \mathrm{Gal}(\mathbb{Q}(t,\zeta)/\mathbb{Q}(t))$ with $\tau(\zeta) = \zeta^2$. We denote by $d_i(t) \in \mathbb{Q}[t]$ the products $d_{i,1}(t)d_{i,2}(t)$. Then one has

$$
\begin{aligned}
d_1(t) &= (t^2+3)(t^2-3t+3),\\
d_2(t) &= t^2-t+1,\\
d_3(t) &= (t^2+3)(t^4+t^3+4t^2+3),\\
d_4(t) &= (t^2-t+1)(t^4-t^3+t^2-3t+3)(t^4+2t^3+4t^2+3t+3).
\end{aligned}
$$

For an odd prime number $p > 3$ we define

$$U_{i,p}(\mathbb{Q}) = \{a \in \mathbb{Q} | v_p(a) < 0 \text{ or } v_p(d_i(a)) \equiv 0 \pmod 3\},$$

and put $U_{i,2}(\mathbb{Q}) = \mathbb{Q}$ for the case $p = 2$. Here v_p is the p-adic valuation. The sets $U_{i,3}(\mathbb{Q})$ are defined to be $U_{i,3}(\mathbb{Q}) = \{a \in \mathbb{Q} | v_3(\mu_i(a)) \geq 1\}$ where $\mu_i(t) \in \mathbb{Q}(t)$ are rational functions such that

$$\mu_i(t) = \frac{(d_{i,1}(t)+d_{i,2}(t))(d_{i,1}(t)-d_{i,2}(t))}{(\zeta^{-1}-\zeta)d_i(t)},$$

respectively.

Proposition 4.11. *For a rational number $a \in \mathbb{Q}$, the conductor* $\mathrm{cond}(L)$ *of the extension $L = \mathrm{Spl}_{\mathbb{Q}} f_i(a,X)$ is equal to $\prod_p p^{r_p}$ where*

$$r_p = \begin{cases} 1 & \text{if } p \neq 3 \text{ and } a \notin U_{i,p},\\ 2 & \text{if } p = 3 \text{ and } a \notin U_{i,3},\\ 0 & \text{otherwise.}\end{cases}$$

For $i = 1,2,3$ and 4 let $h_i \in \mathbb{Q}(\zeta)$ be the squares of the resultants of $d_{i,1}(t)$ and $d_{i,2}(t)$, that is, $h_i = \mathrm{Res}_t(d_{i,1}(t), d_{i,2}(t))^2$. Note that $h_i \in \mathbb{Q}$. In fact, $\tau(h_i) = \mathrm{Res}_t(d_{i,2}(t), d_{i,1}(t))^2 = \mathrm{Res}_t(d_{i,1}(t), d_{i,2}(t))^2 = h_i$. By the direct calculation one sees

Lemma 4.12. *We have $h_1 = 2^2 \cdot 3^6$, $h_2 = -3$, $h_3 = -2^2 \cdot 3^9$ and $h_4 = -3^{19}$.*

Proof of Proposition 4.11. For a rational number $a \in \mathbb{Q}$ let L denote the algebraic number field $\mathrm{Spl}_{\mathbb{Q}} f_i(a,X)$. Let p be a prime number and $\mathfrak{p}$ a prime ideal of $\mathbb{Q}(\zeta)$ above p. It follows from the ramification-conductor theorem that p ramifies in $L/\mathbb{Q}$ if and only if $r_p = v_p(\mathrm{cond}(L)) \geq 1$. Class field theory implies that when $L/\mathbb{Q}$ is ramified at p, we have $r_p = 2$ if $p = 3$ and $r_p = 1$ otherwise. Since the degrees of two cyclic extensions $\mathbb{Q}(\zeta)$ and L of $\mathbb{Q}$ are relatively prime, p ramifies in $L/\mathbb{Q}$ if and only if so does $\mathfrak{p}$ in $L(\zeta)/\mathbb{Q}(\zeta)$. Let us show that $a \in U_{i,p}$ if and only if $\mathfrak{p}$ does not ramify in $L(\zeta)/\mathbb{Q}(\zeta)$. Now denote the ratio $d_{i,1}(a)/d_{i,2}(a)$ by

γ. We first note that 2 does not ramify in any cyclic cubic field. Let us assume $p \geq 5$. If $v_p(a) < 0$, then $v_{\mathfrak{p}}(d_{i,1}(a)) = v_{\mathfrak{p}}(d_{i,2}(a)) < 0$ and $v_{\mathfrak{p}}(\gamma) = 0$ where $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation. Thus it follows from Lemma 4.1 (2) that $L(\zeta)/\mathbb{Q}(\zeta)$ is unramified at $\mathfrak{p}$. Since $v_p(h_i) = 0$, the equation $v_p(d_i(a)) \equiv 0 \pmod 3$ is equivalent to $v_{\mathfrak{p}}(\gamma) \equiv 0 \pmod 3$ under the condition $v_p(a) \geq 0$. Lemma 4.1 (1) and (2) imply that $L(\zeta)/\mathbb{Q}(\zeta)$ is unramified at $\mathfrak{p}$ if and only if $v_p(d_i(a)) \equiv 0 \pmod 3$. Next consider the case $p = 3$. For $\tau(d_{i,1}(a)) = d_{i,2}(a)$ one has $v_{\mathfrak{p}}(\gamma) = 0$. Corollary 4.2 implies that $L(\zeta)/\mathbb{Q}(\zeta)$ is unramified at $\mathfrak{p}$ if and only if $v_{\mathfrak{p}}(\gamma^2 - 1) \geq 3$. Here it holds that $v_{\mathfrak{p}}(\gamma^2 - 1) = v_{\mathfrak{p}}(\gamma - \gamma^{-1}) = v_{\mathfrak{p}}(\mu_i(a)) + 1 = 2v_3(\mu_i(a)) + 1$. Hence $L(\zeta)/\mathbb{Q}(\zeta)$ is unramified at $\mathfrak{p}$ if and only if $v_3(\mu_i(a)) \geq 1$. □

In the same way as above Corollary 4.2 shows

Corollary 4.13. *For a rational number $a \in \mathbb{Q}$ the prime number 3 ramifies, remains prime and splits completely in the extension $\mathrm{Spl}_{\mathbb{Q}} f_i(a, X)/\mathbb{Q}$ provided the valuation $v_3(\mu_i(a))$ is equal to 0, 1 and is greater than 1, respectively.*

Lemma 4.14. *We have*

$$\begin{aligned}
\mu_1(t) &= \frac{3(t-1)(2t^2-3t-3)}{(t^2+3)(t^2-3t+3)},\\
\mu_2(t) &= \frac{2t-1}{t^2-t+1},\\
\mu_3(t) &= \frac{3(t^2+1)(2t^3+t^2+3)}{(t^2+3)(t^4+t^3+4t^2+3)},\\
\mu_4(t) &= \frac{3(t^3+t-1)(2t^5+3t^3-4t^2-3t-3)}{(t^2-t+1)(t^4-t^3+t^2-3t+3)(t^4+2t^3+4t^2+3t+3)}
\end{aligned}$$

and

$$\begin{aligned}
U_{1,3}(\mathbb{Q}) &= \{a \in \mathbb{Q} | v_3(a) \leq 0\},\\
U_{2,3}(\mathbb{Q}) &= \{a \in \mathbb{Q} | v_3(a) \leq -1 \ \text{or}\ v_3(a-5) \geq 2\}.
\end{aligned}$$

The set $U_{3,3}(\mathbb{Q})$ is equal to the set of the rational numbers $a \in \mathbb{Q}$ satisfying one of the disjoint three conditions (i) $v_3(a) \leq -1$, (ii) $v_3(a-2) \geq 1$ *and* (iii) $v_3(a-16) \geq 3$. *The set $U_{4,3}(\mathbb{Q})$ is equal to the set of the rational numbers $a \in \mathbb{Q}$ satisfying one of the disjoint four conditions* (iv) $v_3(a) \leq -1$, (v) $v_3(a-1) \geq 1$, (vi) $v_3(a-2) \geq 2$ *and* (vii) $v_3(a-14) \geq 3$.

Proof. One can directly calculate the invariants $\mu_i(t)$ for $i = 1, 2, 3$ and 4. If $v_3(a) \leq 0$, then $v_3(\mu_1(a)) \geq 1$. When $v_3(a) \geq 1$, one has $v_3(\mu_1(a)) = 0$. Thus we have $U_{1,3}(\mathbb{Q}) = \{a \in \mathbb{Q} | v_3(a) \le 0\}$. If $v_3(a) \le -1$, then $v_3(\mu_2(a)) \ge 1$. When $v_3(a) \ge 1$ or $v_3(a-1) \ge 1$, it holds that $v_3(\mu_2(a)) = 0$. Here one has $\mu_2(2+3t_1) = (2t_1+1)/(3t_1^2+3t_1+1)$. Thus $v_3(a-5) \ge 2$ (resp. $v_3(a-5) = 1$) implies $v_3(\mu_2(a)) \ge 1$ (resp. $v_3(\mu_2(a)) = 0$). This shows that $U_{2,3}(\mathbb{Q}) = \{a \in \mathbb{Q} | v_3(a) \le -1 \text{ or } v_3(a-5) \ge 2\}$.

If $v_3(a) \le -1$, then $v_3(\mu_3(a)) \ge 2$. Here one sees

$$\mu_3(1+3t_1) = \frac{(9t_1^2+6t_1+2)(18t_1^3+21t_1^2+8t_1+2)}{(9t_1^2+6t_1+4)(9t_1^4+15t_1^3+13t_1^2+5t_1+1)},$$

which means that $v_3(\mu_3(a)) = 0$ provided $v_3(a-7) = 1$. By the equation

$$\mu_3(7+9t_2) = \frac{(81t_2^2+126t_2+50)(162t_2^3+387t_2^2+308t_2+82)}{(81t_2^2+126t_2+52)(243t_2^4+783t_2^3+957t_2^2+525t_2+109)},$$

one sees that $v_3(\mu_3(a)) = 0$ if $v_3(a-16) = 2$. When $v_3(a-16) \ge 3$, we have $v_3(\mu_3(a)) \ge 1$. For the case $v_3(a-2) \ge 1$, it holds that $v_3(\mu_3(a)) = 1$. If $v_3(a) \ge 1$, then $v_3(\mu_3(a)) = 0$. Thus we see the assertion for the $U_{3,3}(\mathbb{Q})$.

If $v_3(a) \le -1$, then $v_3(\mu_4(a)) \ge 3$. When $v_3(a-1) \ge 1$, we have $v_3(\mu_4(a)) = 1$. By the direct calculation one sees

$$\begin{aligned}
\mu_4(2+3t_1) = &(9t_1^3+18t_1^2+13t_1+3)(54t_1^5+180t_1^4+249t_1^3+174t_1^2+59t_1+7)\\
&\times(3t_1^2+3t_1+1)^{-1}(9t_1^4+21t_1^3+19t_1^2+7t_1+1)^{-1}\\
&\times(27t_1^4+90t_1^3+120t_1^2+75t_1+19)^{-1},\\
\mu_4(5+9t_2) = &(243t_2^3+405t_2^2+228t_2+43)\\
&\times(4374t_2^5+12150t_2^4+13581t_2^3+7623t_2^2+2144t_2+241)\\
&\times(27t_2^2+27t_2+7)^{-1}\\
&\times(243t_2^4+513t_2^3+408t_2^2+144t_2+19)^{-1}\\
&\times(2187t_2^4+5346t_2^3+4968t_2^2+2079t+331)^{-1}.
\end{aligned}$$

If $v_3(a-2) \ge 2$, then $v_3(\mu_4(a)) \ge 1$. When $v_3(a-8) \ge 2$, we have $v_3(\mu_4(a)) = 0$. For the case $v_3(a-14) \ge 3$ (resp. $v_3(a-14) = 2$), one has $v_3(\mu_4(a)) \ge 1$ (resp. $v_3(\mu_4(a)) = 0$). When $v_3(a) \ge 1$, it holds that $v_3(\mu_4(a)) = 0$. Hence we have verified the assertion for the $U_{4,3}(\mathbb{Q})$. □

§ 5. Two examples of quintic polynomials

Let us consider a quintic polynomial

$$\begin{aligned}
f_5(t,X) = &X^5 + t^2X^4 - 2(t^3+3t^2+5t+5)X^3\\
&+(t^4+5t^3+11t^2+15t+5)X^2 + (t^3+4t^2+10t+10)X + 1,
\end{aligned}$$

which is called the quintic polynomial of Lehmer type [**14**]. The discriminant of the polynomial $f_5(t,X)$ is equal to $(t^3+5t^2+10t+7)^2(t^4+5t^3+15t^2+25t+25)^4$.

Let us denote $\mathrm{Spl}_{\mathbb{Q}(t)} f_5(t,X)$ by L_5 and fix a solution $x_5 \in L_5$ of $f_5(t,X)=0$. Note that $[\mathbb{Q}(t,x_5):\mathbb{Q}(t)]=5$. In fact, a specialized polynomial $f_5(0,X-1)=X^5-5X^4+25X^2-25X+5$ is Eisenstein at the prime number 5. This means that $f_5(t,X)$ is irreducible over $\mathbb{Q}(t)$. It can be checked by a calculator that

$$\begin{aligned}x' = &((t+1)x_5^4+(t^3+2t^2+3t+3)x_5^3-(t+1)(t+2)(t^2+t+4)x_5^2\\ &-(t^4+7t^3+19t^2+29t+19)x_5+(t+1)(t^3+5t^2+11t+9))/\delta_5(t)\end{aligned}$$

is a solution of $f_5(t,X)=0$ where $\delta_5(t)=t^3+5t^2+10t+7$. It follows from $[\mathbb{Q}(t,x_5):\mathbb{Q}(t)]=5$ that $x'\neq x_5$. Thus there exists an element $\sigma_5\in \mathrm{Gal}(L_5/\mathbb{Q}(t))$ such that $\sigma_5(x_5)=x'$. By the direct computation with a calculator it is seen that

$$\begin{aligned}\sigma_5(x_5) = &((t+1)x_5^4+(t^3+2t^2+3t+3)x_5^3-(t+1)(t+2)(t^2+t+4)x_5^2\\ &-(t^4+7t^3+19t^2+29t+19)x_5+(t+1)(t^3+5t^2+11t+9))/\delta_5(t),\\
\sigma_5^2(x_5) = &(-(t+1)(t+2)x_5^4-(t+1)^2(t^2+t-1)x_5^3\\ &+(2t^5+12t^4+33t^3+54t^2+53t+23)x_5^2\\ &-(t+1)(t+2)(t^4+5t^3+12t^2+16+9)x_5\\ &-(t^5+7t^4+24t^3+47t^2+52t+25))/\delta_5(t),\\
\sigma_5^3(x_5) = &(-(2t+3)x_5^4-(2t^3+4t^2+3t+2)x_5^3\\ &+(3t^4+14t^3+31t^2+41t+24)x_5^2\\ &-(t+3)(t^4+4t^3+9t^2+9t+2)x_5-(t+2)(2t+3))/\delta_5(t),\\
\sigma_5^4(x_5) = &((t+2)^2x_5^4+(t+1)(t+2)(t^2+t-1)x_5^3\\ &-(2t^5+14t^4+43t^3+76t^2+80t+39)x_5^2\\ &+(t+1)(t^5+8t^4+29t^3+60t^2+71t+36)x_5\\ &+(t+2)(t^3+6t^2+14t+11))/\delta_5(t)\end{aligned}$$

and $\sigma_5^5(x_5)=x_5$. Thus it holds that $L_5=\mathbb{Q}(t,x_5)$ and $\mathrm{Gal}(L_5/\mathbb{Q}(t))=\langle\sigma_5\rangle\simeq\mathcal{C}_5$. Using Lemma 2.4 it is calculated that 1st Lagrange resolvent y_5 of x_5 for $L_5/\mathbb{Q}(t)$ satisfies

$$\begin{aligned}(5y_5)^5 = &-t^{10}+(5\zeta^3+5\zeta-10)t^9\\ &+(70\zeta^3+10\zeta^2+55\zeta-35)t^8\\ &+(450\zeta^3+125\zeta^2+300\zeta)t^7\\ &+(1775\zeta^3+725\zeta^2+1025\zeta+475)t^6\\ &+(4750\zeta^3+2625\zeta^2+2375\zeta+2125)t^5\\ &+(8875\zeta^3+6500\zeta^2+3750\zeta+5250)t^4\\ &+(11250\zeta^3+11250\zeta^2+3750\zeta+8125)t^3\\ &+(8750\zeta^3+13125\zeta^2+1875\zeta+7500)t^2\\ &+(3125\zeta^3+9375\zeta^2+3125)t+3125\zeta^2\\ = &-(t-\alpha_1)(t-\alpha_2)^3(t-\alpha_3)^2(t-\alpha_4)^4\end{aligned}$$

where ζ is a primitive 5th root of unity in $\overline{\mathbb{Q}}$ and

$$\begin{aligned}\alpha_1 &= -\zeta^3-2\zeta-2, & \alpha_2 &= -2\zeta^2-\zeta-2,\\ \alpha_3 &= -\zeta^3+\zeta^2+\zeta-1, & \alpha_4 &= 2\zeta^3+\zeta^2+2\zeta.\end{aligned}$$

Here α_j are zeros of $t^4+5t^3+15t^2+25t+25=\prod_{j=1}^4(t-\alpha_j)$ and $\tau_j(\alpha_1)=\alpha_j$ where $\tau_j\in \mathrm{Gal}(\mathbb{Q}(t,\zeta))/\mathbb{Q}(t))$ such that $\tau_j(\zeta)=\zeta^j$. We denote the rational function $(t-\alpha_1)(t-\alpha_2)^3(t-\alpha_3)^2(t-\alpha_4)^4\in\mathbb{Q}(t,\zeta)$ by $\lambda_5(t)$. Corollary 2.2 and Proposition 2.6 imply

Proposition 5.1. *We have $L_5(\zeta)=\mathrm{Spl}_{\mathbb{Q}(t,\zeta)}(Y^5-\lambda_5(t))$. In particular, $f_5(t,X)$ is not potentially generic over $\mathbb{Q}$.*

Remark 5.2. Schoof and Washington [**18**] showed that $L_5=\mathbb{Q}(t,x_5)$ is a cyclic quintic extension of $\mathbb{Q}(t)$ whose Galois group $\mathrm{Gal}(L_5/\mathbb{Q}(t))$ is generated by

$$\rho(x_5)=\frac{-x_5^2+tx_5+t+2}{(t+2)x_5+1}.$$

In fact, $\rho=\sigma_5^4\in\mathrm{Gal}(L_5/\mathbb{Q}(t))$. Spearman and Williams [**24**] also gave a generator for $\mathrm{Gal}(L_5/\mathbb{Q}(t))$ whose form is the same as that of σ_5^4 and obtained the same equations on $\sigma_5^j(x_5)$ as above.

Thaine [**25**] gave a quintic polynomial $f_6(t,X)$ such that

$$\begin{aligned}f_6(t,X)=&X^5+(2t^2+5t+10)X^4+(t^4+5t^3+17t^2+25t+25)X^3\\&+(t^4+3t^3+7t^2+5t+5)X^2-(t^3+3t^2+5t+5)X-1.\end{aligned}$$

The discriminant of the polynomial $f_6(t,X)$ is equal to

$$(t^4+4t^3+10t^2+15t+7)^2(t^4+5t^3+15t^2+25t+25)^4.$$

Let us denote $\mathrm{Spl}_{\mathbb{Q}(t)}f_6(t,X)$ by L_6 and fix a solution $x_6\in L_6$ of $f_6(t,X)=0$. In the same way as that of the case $f_5(t,X)$, one can see that $\mathrm{Gal}(L_6/\mathbb{Q}(t))\simeq\mathcal{C}_5$ is generated by σ_6 such that

$$\begin{aligned}\sigma_6(x_6)=&((t+3)x_6^4+(2t^3+10t^2+23t+28)x_6^3\\&+(t^5+6t^4+23t^3+52t^2+68t+54)x_6^2\\&-(t^6+6t^5+23t^4+56t^3+92t^2+99t+42)x_6\\&-(t^6+6t^5+22t^4+52t^3+80t^2+80t+36))/\delta_6(t)\end{aligned}$$

where $\delta_6(t)=t^4+4t^3+10t^2+15t+7$. The 1st Lagrange resolvent y_6 of x_6 for $L_6/\mathbb{Q}(t)$ satisfies

$$(5y_6)^5=\varepsilon^5(t-\alpha_1)^2(t-\alpha_2)(t-\alpha_3)^4(t-\alpha_4)^3$$

where $\varepsilon=\zeta^3+\zeta^2+1\in\mathcal{O}_{\mathbb{Q}(\zeta)}^\times$ and the elements α_j are the same as for $f_5(t,X)$.

Proposition 5.3. *We have $L_5=L_6$.*

Proof. By the above argument one has $y_5^2/y_6 \in \mathbb{Q}(t,\zeta)^5$. Corollary 2.2 implies that $L_5(\zeta) = L_6(\zeta)$ from Kummer theory. The Galois groups of the extensions $L_i(\zeta)/\mathbb{Q}(t)$ are isomorphic to $\mathcal{C}_5\times\mathcal{C}_4$, respectively. Each $\mathcal{C}_5\times\mathcal{C}_4$-extension $L_i(\zeta)/\mathbb{Q}(t)$ has a unique quintic extension L_i of $\mathbb{Q}(t)$ for $i = 5$ and 6. Thus we see $L_5 = L_6$. □

More precisely than Proposition 5.3 one can obtain an explicit relation between the solutions of $f_5(t,X) = 0$ and $f_6(t,X) = 0$. Let us define polynomials $\theta(X)$ and $\widehat{\theta}(X) \in \mathbb{Q}(t)[X]$ by

$$\begin{aligned}\theta(X) = &((t+1)X^4 + (t^3+2t^2+3t+3)X^3\\ &-(t+1)(t+2)(t^2+t+4)X^2\\ &-(t+3)(t^3+3t^2+5t+4)X - (t^3+4t^2+7t+5))/\delta_5(t),\\ \widehat{\theta}(X) = &((t^2+2t+2)X^4 + (2t^4+9t^3+24t^2+32t+21)X^3\\ &+(t^6+7t^5+29t^4+72t^3+118t^2+119t+57)X^2\\ &+(t^3+3t^2+6t+3)(t^3+3t^2+6t+7)X - (t+3))/\delta_6(t).\end{aligned}$$

Proposition 5.4. *We have*

$$f_5(t,X) = \prod_{m=0}^{4}(X - \widehat{\theta}(\sigma_6^m(x_6))), \quad f_6(t,X) = \prod_{m=0}^{4}(X - \theta(\sigma_5^m(x_5))),$$

$\widehat{\theta}\circ\theta(x_5) = x_5$ *and* $\theta\circ\widehat{\theta}(x_6) = x_6$. *In the Galois extension* $L_5 = L_6$ *of* $\mathbb{Q}(t)$, *the action of* σ_5 *is equivalent to that of* σ_6^2.

Proof. Let $\widetilde{\tau_j} \in \mathrm{Gal}(L_5L_6(\zeta)/\mathbb{Q}(t))$ be an extension of $\tau_j \in \mathrm{Gal}(\mathbb{Q}(t,\zeta)/\mathbb{Q}(t))$ such that $\widetilde{\tau_j}(\zeta) = \tau_j(\zeta) = \zeta^j$ and $\widetilde{\tau_j}(x_i) = x_i$ for $i = 5$ and 6. By the argument above one has that $y_6^5 = -\varepsilon^5\widetilde{\tau_2}(y_5)^5$. This means that $y_6 = -\zeta^b\varepsilon\widetilde{\tau_2}(y_5)$ for an integer $b \in \mathbb{Z}$. Let $\widetilde{\sigma_i} \in \mathrm{Gal}(L_i(\zeta)/\mathbb{Q}(t))$ be an extension of $\sigma_i \in \mathrm{Gal}(L_i/\mathbb{Q}(t))$ such that $\widetilde{\sigma_i}(x_i) = \sigma_i(x_i)$ and $\widetilde{\sigma_i}(\zeta) = \zeta$ for $i = 5$ and 6, respectively. Then it holds that $\widetilde{\sigma_i}\widetilde{\tau_j} = \widetilde{\tau_j}\widetilde{\sigma_i}$ as the actions on $L_i(\zeta)$. Lemma 2.1 implies that $\widetilde{\sigma_6}(y_6) = \zeta y_6$. Thus one has $\widetilde{\sigma_6}^{-b+1}(y_6) = -\zeta\varepsilon\widetilde{\tau_2}(y_5)$. Let us put $\eta_5 = -\zeta\varepsilon\widetilde{\tau_2}(y_5)$ and $\eta_6 = \widetilde{\sigma_6}^{-b+1}(y_6)$. It follows from the definition that $\sum_{j=1}^4\widetilde{\tau_j}(y_i) = 4x_i/5 - \sum_{m=1}^4\sigma_i^m(x_i)/5 = x_i - T_i(x_i)/5$ where $T_i(x_i) = \sum_{m=0}^4\sigma_i^m(x_i) \in \mathbb{Q}(t)$. Since $\widetilde{\tau_j}\widetilde{\sigma_i}(y_i) = \widetilde{\sigma_i}\widetilde{\tau_j}(y_i)$, it satisfies that

$$\sum_{j=1}^4\widetilde{\tau_j}(\widetilde{\sigma_i}^m(y_i)) = \sigma_i^m(x_i) - T_i(x_i)/5$$

for an integer $m \in \mathbb{Z}$. This shows that $\sum_{j=1}^4\widetilde{\tau_j}(\eta_6) = \sigma_6^{-b+1}(x_6) - T_6(x_6)/5$. Here it is seen that $\eta_5 = \widetilde{\tau_2}(-\zeta^3(\zeta^4+\zeta+1)y_5) = \widetilde{\tau_2}((\zeta+1)y_5) = \widetilde{\tau_2}(y_5+\widetilde{\sigma_5}(y_5))$. Thus we have $\sum_{j=1}^4\widetilde{\tau_j}(\eta_5) = x_5 + \sigma_5(x_5) - 2T_5(x_5)/5$. Hence the element $\widetilde{\sigma_6}^{-b+1}(x_6)$

is equal to $x_5 + \sigma_5(x_5) - 2T_5(x_5)/5 + T_6(x_6)/5 = \theta(x_5)$ where $T_5(x_5) = -t^2$ and $T_6(x_6) = -(2t^2+5t+10)$. Since $\widetilde{\sigma_6}^{-b+1}(x_6)$ is a solution of $f_6(t,X) = 0$, so is $\theta(x_5)$. Note that $f_6(t,X)$ and $\theta(X)$ are defined over $\mathbb{Q}(t)$. Thus $\sigma_5^m\theta(x_5) = \theta(\sigma_5^m(x_5))$ are also solutions of $f_6(t,X) = 0$. If $\sigma_5^{m_1}\theta(x_5) = \sigma_5^{m_2}\theta(x_5)$ for $0 \leq m_1 < m_2 \leq 4$, then $f_6(t,X)$ is reducible over $\mathbb{Q}(t)$, which is a contradiction. This means that $f_6(t,X) = \prod_{m=0}^4(X - \theta(\sigma_5^m(x_5)))$ and $L_6 \subseteq L_5$. In the same way as above one can find $\widehat{\theta}(X) \in \mathbb{Q}(t)[X]$ such that $f_5(t,X) = \prod_{m=0}^4(X - \widehat{\theta}(\sigma_6^m(x_6)))$ and $\widehat{\theta}\circ\theta(x_5) = x_5$. Thus we prove $L_5 = L_6$. It satisfies that $\theta\circ\widehat{\theta}\circ\theta(x_5) = \theta(x_5)$ and $\theta\circ\widehat{\theta}(\sigma_6^{-b+1}(x_6)) = \sigma_6^{-b+1}(x_6)$. Since $\theta(X)$ and $\widehat{\theta}(X)$ are defined over $\mathbb{Q}(t)$, we have $\theta\circ\widehat{\theta}(x_6) = x_6$. Note that $\widetilde{\sigma_5}^m(\eta_5) = -\zeta\varepsilon\widetilde{\tau_2}(\widetilde{\sigma_5}^m(y_5)) = -\zeta\varepsilon\widetilde{\tau_2}(\zeta^m y_5) = -\zeta\varepsilon\zeta^{2m}\widetilde{\tau_2}(y_5) = \zeta^{2m}\eta_5$. On the other hand, one has $\widetilde{\sigma_6^m}(\eta_6) = \zeta^m\eta_6$. This means that $\sigma_5 = \sigma_6^2$ as the actions on $L_5 = L_6$. □

Remark 5.5. There exist five pairs $(\theta(X), \widehat{\theta}(X))$ satisfying all of the equations in Proposition 5.4. We give a pair which is calculated by using $\sigma_5(x_5)$.

Let us denote $t^4 + 5t^3 + 15t^2 + 25t + 25 = \prod_{j=1}^4(t - \alpha_j)$ by $d(t)$. For an odd prime number $p > 5$ we define

$$U_p(\mathbb{Q}) = \{a \in \mathbb{Q} | v_p(a) < 0 \text{ or } v_p(d(a)) \equiv 0 \pmod 5\},$$

and put $U_2(\mathbb{Q}) = U_3(\mathbb{Q}) = \mathbb{Q}$ for the cases $p = 2$ and 3, respectively. The set $U_5(\mathbb{Q})$ is defined to be $U_5(\mathbb{Q}) = \{a \in \mathbb{Q} | v_5(a) \leq 0\}$.

Proposition 5.6 (Spearman-Williams [**23**]). *For a rational number $a \in \mathbb{Q}$ the conductor of the extension* $\mathrm{Spl}_{\mathbb{Q}} f_5(a,X) = \mathrm{Spl}_{\mathbb{Q}} f_6(a,X)$ *is equal to* $\prod_p p^{r_p}$ *where*

$$r_p = \begin{cases} 1 & \text{if } p \neq 5 \text{ and } a \notin U_p, \\ 2 & \text{if } p = 5 \text{ and } a \notin U_5, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. In the same way as that in the proof of Proposition 4.11 one can show the assertion for the case $p \neq 5$. In fact, it is seen that $\mathrm{disc}_t d(t) = \prod_{1\leq j_1<j_2\leq 4}(\alpha_{j_1} - \alpha_{j_2})^2 = 5^7$. Let us denote $(a-\alpha_1)(a-\alpha_2)^{-2}(a-\alpha_3)^2(a-\alpha_4)^{-1} \in \mathbb{Q}(\zeta)$ by γ. Then one has that $N_{\langle\tau_4\rangle}(\gamma) = 1$ and $v_{\mathfrak{p}}(\gamma) = 0$ where τ_4 is an element of order 2 in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\tau_4(\zeta) = \zeta^4$. Corollary 4.2 implies that $L(\zeta)/\mathbb{Q}(\zeta)$ is

unramified at $\mathfrak{p} = (\zeta - 1)$ if and only if $v_{\mathfrak{p}}(\gamma^2 - 1) \geq 5$. Now put $\mu = (\gamma - \gamma^{-1})/(\zeta - \zeta^{-1})$. Then it holds that $v_{\mathfrak{p}}(\gamma^2 - 1) = v_{\mathfrak{p}}(\gamma - \gamma^{-1}) = v_{\mathfrak{p}}(\mu) + 1$. One can calculate $\mu\tau_2(\mu) = \widetilde{\mu} \in \mathbb{Q}$ where $\tau_2(\zeta) = \zeta^2$ and

$$\widetilde{\mu} = -\frac{5^2(a^4 + 6a^3 + 14a^2 + 15a + 5)(4a^6 + 30a^5 + 65a^4 - 200a^2 - 125a + 125)}{(a^4 + 5a^3 + 15a^2 + 25a + 25)^3}.$$

Here it satisfies that $v_{\mathfrak{p}}(\gamma^2 - 1) = 2v_5(\widetilde{\mu}) + 1$. If $v_5(a) \leq -1$, then $v_5(\widetilde{\mu}) \geq 4$. When $v_5(a - 2) \geq 1$, one has $v_5(\widetilde{\mu}) \geq 3$. For the case $v_5(a) = v_5(a - 2) = 0$, we have $v_5(\widetilde{\mu}) = 2$. The condition $v_5(a) \geq 1$ implies that $v_5(\widetilde{\mu}) = 0$. Hence $L/\mathbb{Q}$ is ramified at 5 if and only if $v_5(a) \geq 1$. □

By the argument in the proof of Proposition 5.6 one sees

Corollary 5.7. *For a rational integer $a \in \mathbb{Q}$, the prime number* 5

$$\begin{cases} \textit{ramifies} & \textit{if } v_5(a) \geq 1, \\ \textit{remains prime} & \textit{if } v_5(a) = v_5(a-2) = 0, \\ \textit{splits completely} & \textit{otherwise}, \end{cases}$$

in the extension $\mathrm{Spl}_{\mathbb{Q}} f_5(a, X)/\mathbb{Q}$.

References

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

[2] H. Cohen, Advanced topics in computational number theory, Grad. Texts in Math. **193**, 2000.

[3] A. Fröhlich, M.J. Taylor, Algebraic number theory, Cambridge Stud. Adv. Math. **27**, 1993.

[4] K. Hashimoto, K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications (Kyoto, 1997), 165–181, Dev. Math. **2**, Kluwer Acad. Publ., Dordrecht, 1999.

[5] K. Hashimoto, Y. Rikuna, *On generic families of cyclic polynomials with even degree*, Manuscripta Math. **107** (2002), no. 3, 283–288.

[6] A. Hoshi, *Noether's problem for some meta-abelian groups of small degree*, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 1, 1–6.

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

[8] G. Kemper, *A constructive approach to Noether's problem*, Manuscripta Math. **90** (1996), no. 3, 343–363.

[9] G. Kemper, E. Mattig, *Generic polynomials with few parameters*, J. Symbolic Comput. **30** (2000), no. 6, 843–857.

[10] Y. Kishi, *A family of cyclic cubic polynomials whose roots are systems of fundamental units*, J. Number Theory **102** (2003), no. 1, 90–106.

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

[12] O. Lecacheux, *Units in number fields and elliptic curves*, Advances in number theory, Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, 293–301.

[13] A. Ledet, *Generic polynomials for Q_8-, QC-, and QQ-extensions*, J. Algebra **237** (2001), no. 1, 1–13.

[14] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), no. 182, 535–541.

[15] S. Nakano, *On generic cyclic polynomials of odd prime degree*, Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), no. 10, 159–162.
[16] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. **130** (2002), no. 8, 2215–2218.
[17] 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.
[18] R. Schoof, L.C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), no. 182, 543–556.
[19] J.-P. Serre, Local fields, Grad. Texts in Math. **67**, 1979.
[20] J.P. Serre, Topics in Galois theory, Res. Notes in Math. **1**, 1992.
[21] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.
[22] G. W. Smith, *Generic cyclic polynomials of odd degree*, Comm. Algebra **19** (1991), no. 12, 3367–3391.
[23] B.K. Spearman, K.S. Williams, *The discriminant of a cyclic field of odd prime degree*, Rocky Mountain J. Math. **33** (2003), no. 3, 1101–1122.
[24] B.K. Spearman, K.S. Williams, *Normal integral bases for Emma Lehmer's parametric family of cyclic quintics*, J. Théor. Nombres Bordeaux **16** (2004), no. 1, 215–220.
[25] F. Thaine, *Finding families of units of cyclic fields*, Algebraic number theory and related topics (Kyoto, 2004). Surikaisekikenkyusho Kokyuroku **1451** (2005), 207–215.
[26] L.C. Washington, *A family of cubic fields and zeros of* 3*-adic* L*-functions*, J. Number Theory **63** (1997), no. 2, 408–417.

(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

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

MHF2005-12 Masayuki UCHIDA & Nakahiro YOSHIDA
AIC for ergodic diffusion processes from discrete observations

MHF2005-13 Hiromichi GOTO & Kenji KAJIWARA
Generating function related to the Okamoto polynomials for the Painlevé IV equation

MHF2005-14 Masato KIMURA & Shin-ichi NAGATA
Precise asymptotic behaviour of the first eigenvalue of Sturm-Liouville problems with large drift

MHF2005-15 Daisuke TAGAMI & Masahisa TABATA
Numerical computations of a melting glass convection in the furnace

MHF2005-16 Raimundas VIDŪNAS
Normalized Leonard pairs and Askey-Wilson relations

MHF2005-17 Raimundas VIDŪNAS
Askey-Wilson relations and Leonard pairs

MHF2005-18 Kenji KAJIWARA & Atsushi MUKAIHIRA
Soliton solutions for the non-autonomous discrete-time Toda lattice equation

MHF2005-19 Yuu HARIYA
Construction of Gibbs measures for 1-dimensional continuum fields

MHF2005-20 Yuu HARIYA
Integration by parts formulae for the Wiener measure restricted to subsets in $\mathbb{R}^d$

MHF2005-21 Yuu HARIYA
A time-change approach to Kotani's extension of Yor's formula

MHF2005-22 Tadahisa FUNAKI, Yuu HARIYA & Mark YOR
Wiener integrals for centered powers of Bessel processes, I

MHF2005-23 Masahisa TABATA & Satoshi KAIZU
Finite element schemes for two-fluids flow problems

MHF2005-24 Ken-ichi MARUNO & Yasuhiro OHTA
Determinant form of dark soliton solutions of the discrete nonlinear Schrödinger equation

MHF2005-25 Alexander V. KITAEV & Raimundas VIDŪNAS
Quadratic transformations of the sixth Painlevé equation

MHF2005-26 Toru FUJII & Sadanori KONISHI
Nonlinear regression modeling via regularized wavelets and smoothing parameter selection

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