RIMS Kôkyûroku Bessatsu
B12 (2009), 223–230

Construction of cyclic number fields with prime degree and their Frobenius automorphisms

By

Toru Komatsu*

§ 1. Introduction

Generic polynomials are solutions of inverse Galois problem. Generic polynomials are used for the constructions of extension fields, e.g., class fields. In this paper we study the Galois actions and the Frobenius automorphisms of specialization fields of a generic cyclic polynomial given by Cohen [1] and Nakano [4]. Let G be a finite group and k a field. We denote by $k(\mathfrak{t})[X]$ the polynomial ring in one variable X whose coefficient ring is the rational function field $k(\mathfrak{t})$ over k with parameters $\mathfrak{t} = (t_1, t_2, \ldots, t_r)$. For a monic polynomial $f(\mathfrak{t}, X) \in k(\mathfrak{t})[X]$ we say that $f(\mathfrak{t}, X)$ is a G-polynomial if the minimal splitting field $\mathrm{Spl}_{k(\mathfrak{t})} f(\mathfrak{t}, X)$ of $f(\mathfrak{t}, X)$ over $k(\mathfrak{t})$ is a Galois G-extension of $k(\mathfrak{t})$. For a G-polynomial $f(\mathfrak{t}, X) \in k(\mathfrak{t})[X]$ and an extension field K of k we say that $f(\mathfrak{t}, X)$ is K-parametric if all Galois G-extensions L of K are realized as specialization fields $\mathrm{Spl}_K f(\mathfrak{s}, X)$ in some $\mathfrak{s} = (s_1, s_2, \ldots, s_r)$, $s_i \in K$. For a G-polynomial $f(\mathfrak{t}, X) \in k(\mathfrak{t})[X]$ we say that $f(\mathfrak{t}, X)$ is k-generic if $f(\mathfrak{t}, X)$ is K-parametric for every extension field K of k with $\sharp K = \infty$. First we introduce the cyclic polynomial of Cohen [1] and Nakano [4]. Let l be an odd prime number and $\mathcal{C}_l$ the cyclic group of order l. Let k be a field whose characteristic is not equal to l. There exists a primitive lth root of unity $\zeta = \zeta_l$ in $\bar{k}$. Let d be the degree of the extension $k(\zeta)/k$. We take d parameters $t_1, t_2, \ldots, t_d$ and use them as a d-tuple $\mathfrak{t} = (t_1, t_2, \ldots, t_d)$. Let Δ be the Galois group $\mathrm{Gal}(k(\mathfrak{t}, \zeta)/k(\mathfrak{t}))$ and σ_i the elements of Δ such that $\sigma_i(\zeta) = \zeta^i$. One has $\Delta \simeq \mathcal{C}_d$. We define an element ε of the group ring $\mathbb{F}_l[\Delta]$ by

$$\varepsilon = \varepsilon_\Delta = \frac{1}{d} \sum_{\sigma_i \in \Delta} \chi(\sigma_i)^{-1} \sigma_i$$

Received April 1, 2008. Revised August 20, 2008.
2000 Mathematics Subject Classification(s): 11R20, 12E10, 12G05.
Key Words: *Generic polynomial, Kummer theory, Artin symbol.*

*Faculty of Science and Technology, Sophia University, Tokyo 102-8554, Japan.
e-mail: trkomatu_math@yahoo.co.jp

where χ is a character of Δ such that $\chi : \Delta \to \mathbb{F}_l^\times$, $\sigma_i \mapsto i$. Note that $\varepsilon^2 = \varepsilon$ in $\mathbb{F}_l[\Delta]$. Now put $e = \sum_{\sigma_i \in \Delta} c_i \sigma_i \in \mathbb{Z}[\Delta]$ where c_i are integers satisfying $dic_i \equiv 1 \pmod{l}$ and $0 < c_i < l$. Then e is a lift of ε, that is, an inverse image of ε by the canonical surjection $\mathbb{Z}[\Delta] \to \mathbb{F}_l[\Delta]$. Let η_j, $j = 1, 2, \ldots, d$ be a basis of $k(\zeta)$ as a k-module. Let $a(\mathfrak{t})$ be a linear form $\sum_{j=1}^{d} t_j \eta_j \in k(\mathfrak{t}, \zeta)$ over $k(\zeta)$. Then one has $e(a(\mathfrak{t})) \in k(\mathfrak{t}, \zeta)$. Let A be an element in the algebraic closure field of $k(\mathfrak{t}, \zeta)$ such that $A^l = e(a(\mathfrak{t}))$. It follows from the property of ε that $k(\mathfrak{t}, \zeta, A)/k(\mathfrak{t})$ is a Galois $(\mathcal{C}_l \times \mathcal{C}_d)$-extension. The group $\mathcal{C}_l \times \mathcal{C}_d$ is cyclic of order ld since d is a divisor of $l - 1$. The Galois group $\mathrm{Gal}(k(\mathfrak{t}, \zeta, A)/k(\mathfrak{t}))$ has a unique subgroup H of order d. We define a polynomial $f(\mathfrak{t}, X) = F(a(\mathfrak{t}), X)$ by

$$f(\mathfrak{t}, X) = F(a(\mathfrak{t}), X) = \prod_{j=0}^{l-1} (X - \mathrm{Tr}_H(\zeta^j A))$$

where $\mathrm{Tr}_H(z) = \sum_{\sigma \in H} \sigma(z)$ for $z \in k(\mathfrak{t}, \zeta, A)$. The polynomial $f(\mathfrak{t}, X)$ is invariant under the actions of $\mathrm{Gal}(k(\mathfrak{t}, \zeta, A)/k(\mathfrak{t}))$. Hence $f(\mathfrak{t}, X) \in k(\mathfrak{t})[X]$.

Proposition 1.1 (Cohen [1]). *The polynomial $f(\mathfrak{t}, X)$ is a k-parametric and $\mathcal{C}_l$-polynomial.*

Proposition 1.2 (Nakano [4]). *The polynomial $f(\mathfrak{t}, X)$ is k-generic.*

If $k = \mathbb{Q}(\zeta_l)$, then $e = \sigma_1$, $a(\mathfrak{t}) = t_1$ and $f(t_1, X) = F(t_1, X) = X^l - t_1$, which is the well-known Kummer polynomial. When $l = 3$ and $k = \mathbb{Q}$, we may have $e = 2\sigma_1 + \sigma_2$ and $a(\mathfrak{t}) = t_1\zeta + t_2\zeta^2$. Then $f(t_1, t_2, X) = F(t_1\zeta + t_2\zeta^2, X)$ is equal to

$$\begin{aligned} &X^3 - 3(t_1^2 - t_1t_2 + t_2^2)X + (t_1 + t_2)(t_1^2 - t_1t_2 + t_2^2) \\ =&X^3 - 3N(a)X - \mathrm{Tr}(a)N(a) \end{aligned}$$

where $a = a(\mathfrak{t})$, $N(z) = \prod_{\sigma \in \Delta} \sigma(z)$ and $\mathrm{Tr}(z) = \sum_{\sigma \in \Delta} \sigma(z)$ for $z \in k(\mathfrak{t}, \zeta)$. When $l = 5$ and $k = \mathbb{Q}$, one may have $e = 4\sigma_1 + 2\sigma_2 + 3\sigma_3 + \sigma_4$ and $a(\mathfrak{t}) = t_1\zeta + t_2\zeta^2 + t_3\zeta^3 + t_4\zeta^4$. Then it is calculated that

$$\begin{aligned} f(\mathfrak{t}, X) = F(a(\mathfrak{t}), X) = &X^5 - 10N(a)X^3 - 5N(a)\mathrm{Tr}(a_1a_2)X^2 \\ &-5N(a)(\mathrm{Tr}(a_1^2a_2a_3) - N(a))X - N(a)\mathrm{Tr}(a_1^3a_2a_3^2) \end{aligned}$$

where $a = a(\mathfrak{t})$, $a_i = \sigma_i(a)$, $N(z) = \prod_{\sigma \in \Delta} \sigma(z)$ and $\mathrm{Tr}(z) = \sum_{\sigma \in \Delta} \sigma(z)$ for $z \in k(\mathfrak{t}, \zeta)$. In the same way as above, if $l = 7$ and $k = \mathbb{Q}$, then $e = 6\sigma_1 + 3\sigma_2 + 2\sigma_3 + 5\sigma_4 + 4\sigma_5 + \sigma_6$

and $f(\mathfrak{t}, X) = F(a(\mathfrak{t}), X)$ is equal to

$$\begin{aligned}F(a(\mathfrak{t}), X) = {} & X^7 - 21N(a)X^5 - 7N(a)(\mathrm{Tr}(a_1a_2a_3) + 2\mathrm{Tr}(a_1a_2a_4)/3)X^4 \\ & -7N(a)(\mathrm{Tr}(a_1^2a_2^2a_3a_4) + 3\mathrm{Tr}(a_1^2a_2a_3a_4a_5) - 9N(a))X^3 \\ & -7N(a)(2\mathrm{Tr}(a_1^3a_2^2a_3a_4^2a_5) + \mathrm{Tr}(a_1^3a_2a_3a_4^2a_5^2) \\ & \qquad +N(a)(\mathrm{Tr}(a_1a_2a_3) - 2\mathrm{Tr}(a_1a_2a_4)))X^2 \\ & -7N(a)(\mathrm{Tr}(a_1^4a_2^2a_3a_4^3a_5^2) - N(a)(\mathrm{Tr}(a_1^2a_2^2a_3^2) - \mathrm{Tr}(a_1^2a_2^2a_4^2)/3 \\ & \qquad -3\mathrm{Tr}(a_1^2a_2a_3^2a_5) + 4\mathrm{Tr}(a_1^2a_2a_3a_4a_5) - 9N(a)))X \\ & -N(a)(\mathrm{Tr}(a_1^5a_2^2a_3a_4^4a_5^3) - 7N(a)(\mathrm{Tr}(a_1^3a_2^3a_3^2a_4) - \mathrm{Tr}(a_1^3a_2^3a_3a_4^2) \\ & \qquad -2\mathrm{Tr}(a_1^3a_2^2a_3^2a_4a_5) + 3\mathrm{Tr}(a_1^3a_2^2a_3a_4^2a_5) + \mathrm{Tr}(a_1^3a_2a_3^2a_4a_5^2) \\ & \qquad -2\mathrm{Tr}(a_1^3a_2a_3a_4^2a_5^2) + 2N(a)(\mathrm{Tr}(a_1a_2a_3) - \mathrm{Tr}(a_1a_2a_4))))\end{aligned}$$

where $a = a(\mathfrak{t})$, $a_i = \sigma_i(a)$, $N(z) = \prod_{\sigma\in\Delta}\sigma(z)$ and $\mathrm{Tr}(z) = \sum_{\sigma\in\Delta}\sigma(z)$ for $z \in k(\mathfrak{t}, \zeta)$.

In this paper we study the arithmetic of the polynomial $f(\mathfrak{t}, X)$, in particular, the Galois actions and the Frobenius automorphisms of the specialization fields over a number field. In the section 2 we study explicit Galois actions in the Galois extension $\mathrm{Spl}_{k(\mathfrak{t})}f(\mathfrak{t}, X)$ of $k(\mathfrak{t})$ (Proposition 2.1). In the section 3 we introduce a group S to solve the subfield problem of the generic polynomial $f(\mathfrak{t}, X)$ (Proposition 3.3). In the section 4, by using the group S, we study the Frobenius automorphisms of the specialization fields over a finite number field (Theorem 4.1). In the section 5 we study an evolution of the generic polynomial to decrease the number of the parameters and to succeed the genericity (Corollary 5.5).

§ 2. Global action

In this section we study the explicit Galois actions of the Galois extension defined by the cyclic polynomial of Cohen and Nakano. Let $f(\mathfrak{t}, X)$ be the $\mathcal{C}_l$-polynomial of Cohen and Nakano in the introduction with $k = \mathbb{Q}$. For an integer $j \in \mathbb{Z}$ we denote by x_j the zero $\mathrm{Tr}_H(\zeta^j A)$ of the polynomial $f(\mathfrak{t}, X)$. Since $\mathrm{Spl}_{\mathbb{Q}(\mathfrak{t})}f(\mathfrak{t}, X)$ is a cyclic extension of $\mathbb{Q}(\mathfrak{t})$ with degree l, there exist rational functions $\lambda_{ij} \in \mathbb{Q}(\mathfrak{t})$ such that $x_i = \sum_{j=0}^{l-1}\lambda_{ij}x_0^j$. We define the three $(l\times l)$-matrices Λ, C and V by $\Lambda = (\lambda_{ij})$, $C = (x_{i+j})$ and $V = (x_j^i)$ where the indices i and j run through the integers from 0 to $l-1$. Note that $x_{m+l} = x_m$ for every $m \in \mathbb{Z}$. Here C is a circle matrix and V is a Vandermonde matrix.

Proposition 2.1. *We have* $\Lambda = CV^{-1}$.

Proof. It follows from the definition that $C = \Lambda V$. Since the zeros x_j of $f(\mathfrak{t}, X)$ are distinct, the matrix V is invertible. Thus it satisfies $\Lambda = CV^{-1}$. □

For example, when $l = 3$ and $k = \mathbb{Q}$, we may have $e = 2\sigma_1 + \sigma_2$ and $a(\mathfrak{t}) = t_1\zeta + t_2\zeta^2$.

Proposition 2.1 implies that

$$\Lambda = \begin{bmatrix} 0 & 1 & 0 \\ \dfrac{2(t_1^2 - t_1t_2 + t_2^2)}{t_1 - t_2} & -\dfrac{t_1}{t_1 - t_2} & -\dfrac{1}{t_1 - t_2} \\ -\dfrac{2(t_1^2 - t_1t_2 + t_2^2)}{t_1 - t_2} & \dfrac{t_2}{t_1 - t_2} & \dfrac{1}{t_1 - t_2} \end{bmatrix}.$$

This shows that

$$\begin{aligned} x_1 &= -\frac{1}{t_1 - t_2}x_0^2 - \frac{t_1}{t_1 - t_2}x_0 + \frac{2(t_1^2 - t_1t_2 + t_2^2)}{t_1 - t_2}, \\ x_2 &= \frac{1}{t_1 - t_2}x_0^2 + \frac{t_2}{t_1 - t_2}x_0 - \frac{2(t_1^2 - t_1t_2 + t_2^2)}{t_1 - t_2}. \end{aligned}$$

§ 3. Group structure

In this section we define a group to solve the subfield problem of the generic polynomial $f(\mathfrak{t}, X)$. Let us assume that $k = \mathbb{Q}$ and $a(\mathfrak{t}) = \sum_{j=1}^{l-1} t_j\zeta^j$. Recall that $e = \sum_{i=1}^{l-1} c_i\sigma_i \in \mathbb{Z}[\Delta]$ where $-ic_i \equiv 1 \pmod{l}$ and $0 < c_i < l$. For an integer i with $0 < i < l$ we denote the linear form $\sigma_i(a(\mathfrak{t}))$ by $a_i(\mathfrak{t})$ and the polynomial $e(a_i(\mathfrak{t})) \in \mathbb{Q}(\zeta)[\mathfrak{t}]$ by $g_i(\mathfrak{t})$. We denote $(a_i(\mathfrak{t}))_{i=1}^{l-1}$ by $\mathfrak{a}(\mathfrak{t})$ and $(g_i(\mathfrak{t}))_{i=1}^{l-1}$ by $\mathfrak{g}(\mathfrak{t})$. We define a subspace S of $\mathbb{A}^{l-1}$ by

$$S = \{\mathfrak{s} = (s_1, s_2, \ldots, s_{l-1}) | a_i(\mathfrak{s}) \neq 0 \text{ for every } i \in \mathbb{Z} \text{ with } 0 < i < l\}.$$

For two elements $\mathfrak{q} = (q_1, q_2, \ldots, q_{l-1})$ and $\mathfrak{r} = (r_1, r_2, \ldots, r_{l-1}) \in S$ we define a composition law $+_S$ on S by $\mathfrak{q} +_S \mathfrak{r} = (s_1, s_2, \ldots, s_{l-1})$ where

$$s_j = \sum_{i=1}^{j-1} q_ir_{j-i} + \sum_{i=j+1}^{l-1} q_ir_{l+j-i} - \sum_{i=1}^{l-1} q_ir_{l-i}$$

with $0 < j < l$. For an integer i with $0 < i < l$ we define a rational function $m_i(\mathfrak{t}) \in \mathbb{Q}(\mathfrak{t})$ by $m_i(\mathfrak{t}) = \mathrm{Tr}_{\mathbb{Q}(\mathfrak{t},\zeta)/\mathbb{Q}(\mathfrak{t})}((\zeta^{-i} - 1)/a_1(\mathfrak{t}))/l$, and denote $(m_i(\mathfrak{t}))_{i=1}^{l-1}$ by $\mathfrak{m}(\mathfrak{t})$.

Lemma 3.1. *The set S is an algebraic torus of dimension $l - 1$ with the composition law $+_S$ and an isomorphism $S \to \mathbb{G}_m^{l-1}$, $\mathfrak{s} \mapsto \mathfrak{a}(\mathfrak{s})$. The identity id_S of S is $(-1, -1, \ldots, -1)$. The inverse element of $\mathfrak{s} \in S$ on $+_S$ is equal to $\mathfrak{m}(\mathfrak{s})$.*

For an integer i with $0 < i < l$ we define a rational function $\hat{g}_i(\mathfrak{t}) \in \mathbb{Q}(\mathfrak{t})$ by $\hat{g}_i(\mathfrak{t}) = \mathrm{Tr}_{\mathbb{Q}(\mathfrak{t},\zeta)/\mathbb{Q}(\mathfrak{t})}((\zeta^{-i} - 1)g_1(\mathfrak{t}))/l$, and denote $(\hat{g}_i(\mathfrak{t}))_{i=1}^{l-1}$ by $\hat{\mathfrak{g}}(\mathfrak{t})$. Note that $\hat{\mathfrak{g}}$ is a map from S to itself.

Lemma 3.2. *We have $\mathfrak{g}(\mathfrak{t}) = \mathfrak{a}(\hat{\mathfrak{g}}(\mathfrak{t}))$.*

Let K be an extension field of $\mathbb{Q}$. For a K-valued element $\mathfrak{s} \in S(K)$ of S let $L_{\mathfrak{s}}$ denote the minimal splitting field $\mathrm{Spl}_K f(\mathfrak{s}, X)$ over K of $f(\mathfrak{s}, X) \in K[X]$. For a positive integer n and $\mathfrak{s} \in S$ let $[n](\mathfrak{s})$ denote the sum $\mathfrak{s} +_S \mathfrak{s} +_S \cdots +_S \mathfrak{s}$ with n terms.

Proposition 3.3. *For two elements $\mathfrak{q}$ and $\mathfrak{r} \in S(K)$, the field $L_{\mathfrak{q}}$ is contained in the field $L_{\mathfrak{r}}$ if and only if there exist an integer $j \in \mathbb{Z}$ and an element $\mathfrak{s} \in S(K)$ such that $\hat{\mathfrak{g}}(\mathfrak{q}) = [j]\hat{\mathfrak{g}}(\mathfrak{r}) +_S [l](\mathfrak{s})$.*

For example, when $l = 3$, it is calculated that

$$\begin{gathered} S = \{(s_1, s_2) \in \mathbb{A}^2 | s_1^2 - s_1 s_2 + s_2^2 \neq 0\} \\ (q_1, q_2) +_S (r_1, r_2) = (q_2 r_2 - q_1 r_2 - q_2 r_1, q_1 r_1 - q_1 r_2 - q_2 r_1), \\ \mathrm{id}_S = (-1, -1), \\ \mathfrak{m}(s_1, s_2) = \left(\frac{s_2}{s_1^2 - s_1 s_2 + s_2^2}, \frac{s_1}{s_1^2 - s_1 s_2 + s_2^2} \right), \\ \hat{\mathfrak{g}}(s_1, s_2) = (s_1^3 - s_1^2 s_2 + s_1 s_2^2, s_1^2 s_2 - s_1 s_2^2 + s_2^3). \end{gathered}$$

Remark. For the finite field $\mathbb{F}_p$ of characteristic $p \neq l$, the mod p reduction model $S_{\mathbb{F}_p}$ of the algebraic group S is well-defined.

§ 4. Local action

In this section we study the Frobenius automorphisms of the specialization fields of $f(\mathfrak{t}, X)$ over a finite number field by using the group S. Let K be a finite number field. Let $L_{\mathfrak{s}}$ denote the minimal splitting field $\mathrm{Spl}_K f(\mathfrak{s}, X)$ of $f(\mathfrak{s}, X)$ over K for an element $\mathfrak{s} \in S(K)$. For an integer i let x_i be the zero $\mathrm{Tr}_H(\zeta^i \sqrt[l]{g_1(\mathfrak{s})})$ of the polynomial $f(\mathfrak{s}, X)$. Now assume that $L_{\mathfrak{s}} \neq K$, that is, $[L_{\mathfrak{s}} : K] = l$. Let τ_1 be the generator of $\mathrm{Gal}(L_{\mathfrak{s}}/K)$ where $\tau_1(x_0) = x_1$. Let $\mathfrak{p}$ be a prime ideal of K and $\mathfrak{P}$ a prime ideal of $K(\zeta)$ above $\mathfrak{p}$. Let $\mathbb{F}_{\mathfrak{p}}$ be the residue class field of K at $\mathfrak{p}$ and $\mathbb{F}_{\mathfrak{P}}$ that of $K(\zeta)$ at $\mathfrak{P}$. Now put $d_{\mathfrak{P}} = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_p]$ and $d_{\mathfrak{P}/\mathfrak{p}} = [\mathbb{F}_{\mathfrak{P}} : F_{\mathfrak{p}}]$ where p is the prime number below $\mathfrak{p}$.

Theorem 4.1. *If p is not equal to l and $\mathfrak{s}$ (mod $\mathfrak{p}$) belongs to $S(\mathbb{F}_{\mathfrak{p}})$, then $L_{\mathfrak{s}}/K$ is unramified at $\mathfrak{p}$. In such a case, the Frobenius automorphism $\left(\frac{L_{\mathfrak{s}}/K}{\mathfrak{p}}\right)$ of $\mathfrak{p}$ in the extension $L_{\mathfrak{s}}/K$ is equal to τ_1^j where j is an integer satisfying*

$$\left[\frac{p^{d_{\mathfrak{P}}} - 1}{l}\right] \hat{\mathfrak{g}}(\mathfrak{s}) = [j d_{\mathfrak{P}/\mathfrak{p}}](1, 0, 0, \ldots, 0) \quad \text{in } S(\mathbb{F}_{\mathfrak{p}}).$$

Proof. The condition $\mathfrak{s}$ (mod $\mathfrak{p}$) $\in S(\mathbb{F}_{\mathfrak{p}})$ implies that the additive $\mathfrak{P}$-adic valuation $v_{\mathfrak{P}}(g_1(\mathfrak{s}))$ of $g_1(\mathfrak{s})$ is equal to 0. It follows from $\mathfrak{P} \nmid l$ that $\mathfrak{P}$ is unramified in $L_{\mathfrak{s}}(\zeta)/K(\zeta)$ and so is $\mathfrak{p}$ in $L_{\mathfrak{s}}/K$. For an element $\tau \in \mathrm{Gal}(L_{\mathfrak{s}}/K)$ let $\tilde{\tau}$ be the extension of τ to $\mathrm{Gal}(L_{\mathfrak{s}}(\zeta)/K)$ such that $\tilde{\tau}(\zeta) = \zeta$. It is easily seen that $\tilde{\tau_1}(\sqrt[l]{g_1(\mathfrak{s})}) = \zeta\sqrt[l]{g_1(\mathfrak{s})}$ for $\tilde{\tau_1}(x_i) = x_{i+1}$ and $\tilde{\tau_1}(\zeta) = \zeta$. For an element $\tau \in \mathrm{Gal}(L_{\mathfrak{s}}(\zeta)/K(\zeta))$ let τ_K denote the image of τ by the natural inclusion map $\mathrm{Gal}(L_{\mathfrak{s}}(\zeta)/K(\zeta)) \to \mathrm{Gal}(L_{\mathfrak{s}}(\zeta)/K)$. It is known (cf. Fröhlich-Taylor [3] Theorem 30) that

$$\left(\frac{L_{\mathfrak{s}}(\zeta)/K}{\mathfrak{p}}\right)^{d_{\mathfrak{P}/\mathfrak{p}}} = \left(\frac{L_{\mathfrak{s}}(\zeta)/K(\zeta)}{\mathfrak{P}}\right)_K \quad \text{and} \quad \left.\left(\frac{L_{\mathfrak{s}}(\zeta)/K}{\mathfrak{p}}\right)\right|_{L_{\mathfrak{s}}} = \left(\frac{L_{\mathfrak{s}}/K}{\mathfrak{p}}\right).$$

Now suppose that $\left(\frac{L_{\mathfrak{s}}/K}{\mathfrak{p}}\right) = \tau_1^j$ for some $j \in \mathbb{Z}$. Then one has that $\tau_1^{jd_{\mathfrak{P}/\mathfrak{p}}} = \left.\left(\frac{L_{\mathfrak{s}}(\zeta)/K(\zeta)}{\mathfrak{P}}\right)_K\right|_{L_{\mathfrak{s}}}$. By class field theory, if $g_1(\mathfrak{s})^{(p^{d_{\mathfrak{P}}}-1)/l} \equiv \zeta^{j_1} \pmod{\mathfrak{P}}$ for an integer j_1, then $\left(\frac{L_{\mathfrak{s}}(\zeta)/K(\zeta)}{\mathfrak{P}}\right)_K = \tilde{\tau_1}^{j_1}$. The elements $\tilde{\tau_1}|_{L_{\mathfrak{s}}}$ and τ_1 coincide and have order l. This means that $jd_{\mathfrak{P}/\mathfrak{p}} \equiv j_1 \pmod{l}$. Thus it holds that

$$g_1(\mathfrak{s})^{(p^{d_{\mathfrak{P}}}-1)/l} \equiv \zeta^{jd_{\mathfrak{P}/\mathfrak{p}}} \pmod{\mathfrak{P}}.$$

By the definition of $\hat{\mathfrak{g}}(\mathfrak{t})$ we have

$$\left[\frac{p^{d_{\mathfrak{P}}}-1}{l}\right]\hat{\mathfrak{g}}(\mathfrak{s}) = [jd_{\mathfrak{P}/\mathfrak{p}}](1,0,0,\dots,0) \quad \text{in } S(\mathbb{F}_{\mathfrak{P}}).$$

Here the element $\mathfrak{y} = (1,0,0,\dots,0)$ satisfies $a_i(\mathfrak{y}) = \zeta^i$. Note that $(p^{d_{\mathfrak{P}}}-1)/l$ and $jd_{\mathfrak{P}/\mathfrak{p}}$ are integers, and $\hat{\mathfrak{g}}(\mathfrak{s})$ and $\mathfrak{y}$ are elements in $S(\mathbb{F}_{\mathfrak{p}})$. Thus the equation above holds over $\mathbb{F}_{\mathfrak{p}}$. □

The ramifications at l of the specialization fields of $f(\mathfrak{t}, X)$ over $\mathbb{Q}$ are as follows.

Proposition 4.2. *Let $\mathfrak{s} = (s_1, s_2, \dots, s_{l-1})$ be an element of $S(\mathbb{Q})$ such that $s_i \in \mathbb{Z}_l$ and $\sum_{i=1}^{l-1} s_i \not\equiv 0 \pmod{l}$. Then the extension $\mathrm{Spl}_{\mathbb{Q}} f(\mathfrak{s}, X)$ of $\mathbb{Q}$ is unramified at l if and only if it satisfies $\sum_{i=1}^{l-1} is_i \equiv 0 \pmod{l}$.*

Proof. Let us denote $\mathrm{Spl}_{\mathbb{Q}} f(\mathfrak{s}, X)$ by L. The ramification index of l in $L/\mathbb{Q}$ is equal to that of $\mathfrak{L}$ in $L(\zeta)/\mathbb{Q}(\zeta)$ where $\mathfrak{L} = (1-\zeta)$ is the prime ideal of $\mathbb{Q}(\zeta)$ above l. Now put $n_0 = \sum_{i=1}^{l-1} s_i$. It follows from the assumption that $n_0 \in \mathbb{Z}_l^{\times}$. There exist integer n_1 and a positive integer j such that $a(\mathfrak{s}) \equiv n_0 + n_1(1-\zeta)^j \pmod{\mathfrak{L}^{j+1}}$. One has

$$\begin{aligned} e\left(\frac{a(\mathfrak{s})}{n_0}\right) &\equiv \prod_{i=1}^{l-1}\left(1 - \frac{n(1-\zeta^i)^j}{i}\right) \\ &\equiv \prod_{i=1}^{l-1}(1 - n(1-\zeta)^j i^{j-1}) \\ &\equiv 1 - n(1-\zeta)^j \sum_{i=1}^{l-1} i^{j-1} \pmod{\mathfrak{L}^{j+1}} \end{aligned}$$

where $n = n_1/n_0 \in \mathbb{Z}_l \cap \mathbb{Q}$. Thus, estimating the sum $\sum_{i=1}^{l-1} i^{j-1}$ modulo l, we have

$$e\left(\frac{a(\mathfrak{s})}{n_0}\right) \equiv \begin{cases} 1 + n(1-\zeta) & (j=1), \\ 1 & (2 \le j \le l-1) \end{cases} \pmod{\mathfrak{L}^{j+1}}.$$

If $j = 1$ and $n_1 \not\equiv 0 \pmod{l}$, then $e(a(\mathfrak{s})/n_0) \equiv 1 \pmod{\mathfrak{L}}$ and $e(a(\mathfrak{s})/n_0) \not\equiv 1 \pmod{\mathfrak{L}^2}$. This means that $\mathfrak{L}$ ramifies in $L_{\mathfrak{s}}(\zeta)/\mathbb{Q}(\zeta)$. In fact, $\mathrm{Spl}_{\mathbb{Q}} F(a(\mathfrak{s}), X) = \mathrm{Spl}_{\mathbb{Q}} F(a(\mathfrak{s})/n_0, X)$ for $e(n_0) \in \mathbb{Q}(\zeta)^{\times l}$. When $j \ge 2$, we see that $e(a(\mathfrak{s})/n_0) \equiv 1 \pmod{\mathfrak{L}^l}$ by using the above congruence, repeatedly. Thus $\mathfrak{L}$ does not ramify in $L_{\mathfrak{s}}(\zeta)/\mathbb{Q}(\zeta)$. Note that $a(\mathfrak{s}) - n_0 = \sum_{i=1}^{l-1}(\zeta^i - 1)s_i \equiv (\zeta - 1)\sum_{i=1}^{l-1} is_i \pmod{\mathfrak{L}^2}$. Hence $L(\zeta)/\mathbb{Q}(\zeta)$ is unramified at $\mathfrak{L}$ if and only if it satisfies $\sum_{i=1}^{l-1} is_i \equiv 0 \pmod{\mathfrak{L}}$. This proves the assertion of the proposition. □

§ 5. Decreasing parameters

In the section 5 we study an evolution of the generic polynomial to decrease the number of the parameters and to succeed the genericity. For an integer $i \in \mathbb{Z}$ we denote $\zeta^i + \zeta^{-i}$ by ω_i and simply ω_1 by ω. For an element $z \in \mathbb{Q}(\mathfrak{t}, \omega)$ we denote the trace $\mathrm{Tr}_{\mathbb{Q}(\mathfrak{t},\omega)/\mathbb{Q}(\mathfrak{t})}(z)$ by $\mathrm{Tr}_\omega(z)$. The following properties of ω_i are easily seen.

Lemma 5.1. *For $1 \le i, j \le (l-1)/2$ we have $\mathrm{Tr}_\omega(\omega_i(\omega_j - 2)) = l\delta_{ij}$ where δ_{ij} is the Kronecker's delta.*

Lemma 5.2. *For an element $z \in \mathbb{Q}(\mathfrak{t}, \omega)$ we have*

$$z = \frac{1}{l}\sum_{i=1}^{(l-1)/2} \mathrm{Tr}_\omega((\omega_i - 2)z)\omega_i.$$

Let $\mathfrak{u}$ be $(l-1)/2$ parameters $u_1, u_2, \ldots, u_{(l-1)/2}$. We denote by $b(\mathfrak{u})$ a polynomial $\zeta + \sum_{i=1}^{(l-1)/2} u_i\omega_i$. In the same way as the definition of $F(a(\mathfrak{t}), X)$ we define $F(b(\mathfrak{u}), X) = \prod_{j=0}^{l-1}(X - \mathrm{Tr}_H(\zeta^j \sqrt[l]{e(b(\mathfrak{u}))}))$, which is written by $h(\mathfrak{u}, X)$. For $1 \le i \le (l-1)/2$ let $\pi_i(\mathfrak{t})$ be rational functions in $\mathbb{Q}(\mathfrak{t})$ such that

$$\pi_i(\mathfrak{t}) = -\frac{1}{l}\mathrm{Tr}_\omega\left((\omega_i - 2)\frac{\zeta^{-1}a(\mathfrak{t}) - \zeta\bar{a}(\mathfrak{t})}{a(\mathfrak{t}) - \bar{a}(\mathfrak{t})}\right)$$

where $\bar{a}(\mathfrak{t}) = \sum_{i=1}^{l-1} t_i\zeta^{-i}$. We denote $(\pi_i(\mathfrak{t}))_{i=1}^{(l-1)/2}$ by $\pi(\mathfrak{t})$.

Lemma 5.3. *We have $b(\pi(\mathfrak{t})) = (\zeta - \zeta^{-1})a(\mathfrak{t})/(a(\mathfrak{t}) - \bar{a}(\mathfrak{t}))$.*

Proof. Since $-(\zeta^{-1}a(\mathfrak{t}) - \zeta\bar{a}(\mathfrak{t}))/(a(\mathfrak{t}) - \bar{a}(\mathfrak{t}))$ belongs to $\mathbb{Q}(\mathfrak{t}, \omega)$, Lemma 5.2 implies that $\sum_{i=1}^{(l-1)/2} \pi_i(\mathfrak{t})\omega_i = -(\zeta^{-1}a(\mathfrak{t}) - \zeta\bar{a}(\mathfrak{t}))/(a(\mathfrak{t}) - \bar{a}(\mathfrak{t}))$. Thus we have $b(\pi(\mathfrak{t})) = \zeta + \sum_{i=1}^{(l-1)/2} \pi_i(\mathfrak{t})\omega_i = (\zeta - \zeta^{-1})a(\mathfrak{t})/(a(\mathfrak{t}) - \bar{a}(\mathfrak{t}))$. □

Proposition 5.4. *We have* $\mathrm{Spl}_{\mathbb{Q}(\mathfrak{t})}h(\pi(\mathfrak{t}),X)=\mathrm{Spl}_{\mathbb{Q}(\mathfrak{t})}f(\mathfrak{t},X)$.

Proof. It follows from Lemma 5.3 that $b(\pi(\mathfrak{t}))/a(\mathfrak{t})=(\zeta-\zeta^{-1})/(a(\mathfrak{t})-\bar{a}(\mathfrak{t}))\in\mathbb{Q}(\mathfrak{t},\omega)^{\times}$. If $z\in\mathbb{Q}(\mathfrak{t},\omega)^{\times}$, then $e(z)\in\mathbb{Q}(\mathfrak{t},\zeta)^{\times l}$. The ratio $e(b(\pi(\mathfrak{t})))/e(a(\mathfrak{t}))$ is an lth power element in $\mathbb{Q}(\mathfrak{t},\zeta)$. Kummer theory shows that $\mathbb{Q}(\mathfrak{t},\zeta,\sqrt[l]{e(a(\mathfrak{t}))})$ and $\mathbb{Q}(\mathfrak{t},\zeta,\sqrt[l]{e(b(\pi(\mathfrak{t})))})$ coincide and so do their subfields $\mathrm{Spl}_{\mathbb{Q}(\mathfrak{t})}F(a(\mathfrak{t}),X)$ and $\mathrm{Spl}_{\mathbb{Q}(\mathfrak{t})}F(b(\pi(\mathfrak{t})),X)$. □

Corollary 5.5. *The polynomial* $h(\mathfrak{u},X)$ *is a* $\mathbb{Q}$*-generic* $\mathcal{C}_l$*-polynomial.*

We can see the arithmetic of $h(\mathfrak{u},X)$ by that of $f(\mathfrak{t},X)$ via the map $\pi$.

Remark. Smith [5] and Dentzer [2] construct cyclic polynomials of odd degree over $\mathbb{Q}$. Smith [5] also gives a generic $\mathcal{C}_l$-polynomial over $\mathbb{Q}$ with $(l-1)/2$ parameters. Smith decreases the number of the parameters by multiplying elements of $\mathbb{Q}(\mathfrak{t},\omega)$ as that for our $h(\mathfrak{u},X)$.

Acknowledgement. The author is very grateful to the organizer Professor Mamoru Asada for giving an opportunity to talk at the conference and to contribute this article. He is grateful to the referee for many helpful comments and careful reading of the manuscript.

References

[1] Cohen, H., *Advanced topics in computational number theory*, Grad. Texts in Math. **193**, Springer-Verlag, New York, 2000.

[2] Dentzer, R., *Polynomials with cyclic Galois group*, Comm. Algebra **23** (1995), 1593–1603.

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

[4] Nakano, S., *On generic cyclic polynomials of odd prime degree*, Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), no. 10, 159–162.

[5] Smith, G.W., *Generic cyclic polynomials of odd degree*, Comm. Algebra **19** (1991), 3367–3391.