<table>
<thead>
<tr>
<th>Title</th>
<th>Construction of cyclic number fields with prime degree and their Frobenius automorphisms (Algebraic Number Theory and Related Topics 2007)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>KOMATSU, Toru</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録別冊 = RIMS Kokyuroku Bessatsu (2009), B12: 223-230</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2009-08</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/176785">http://hdl.handle.net/2433/176785</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>
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 $k(t)[X]$ the polynomial ring in one variable $X$ whose coefficient ring is the rational function field $k(t)$ over $k$ with parameters $t=(t_1, t_2, \ldots, t_r)$. For a monic polynomial $f(t, X) \in k(t)[X]$ we say that $f(t, X)$ is a $G$-polynomial if the minimal splitting field $\text{Spl}_{k(t)}f(t, X)$ of $f(t, X)$ over $k(t)$ is a Galois $G$-extension of $k(t)$. For a $G$-polynomial $f(t, X) \in k(t)[X]$ and an extension field $K$ of $k$ we say that $f(t, X)$ is $K$-parametric if all Galois $G$-extensions $L$ of $K$ are realized as specialization fields $\text{Spl}_Kf(s, X)$ in some $s=(s_1, s_2, \ldots, s_r), s_i \in K$. For a $G$-polynomial $f(t, X) \in k(t)[X]$ we say that $f(t, X)$ is $k$-generic if $f(t, X)$ is $K$-parametric for every extension field $K$ of $k$ with $\#K=\infty$. First we introduce the cyclic polynomial of Cohen [1] and Nakano [4]. Let $l$ be an odd prime number and $C_l$ the cyclic group of order $l$. Let $k$ be a field whose characteristic is not equal to $l$. There exists a primitive $l$th root of unity $\zeta = \zeta_l$ in $k$. 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 $t=(t_1, t_2, \ldots, t_d)$. Let $\Delta$ be the Galois group $\text{Gal}(k(t, \zeta)/k(t))$ and $\sigma_i$ the elements of $\Delta$ such that $\sigma_i(\zeta) = \zeta^i$. One has $\Delta \simeq C_d$. We define an element $\varepsilon$ of the group ring $\mathbb{F}_l[\Delta]$ by

$$\varepsilon = \varepsilon_\Delta = \frac{1}{d} \sum_{\sigma_i \in \Delta} \chi(\sigma_i)^{-1}\sigma_i$$
where $\chi$ is a character of $\Delta$ 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 $d c_i \equiv 1 \pmod{l}$ and $0 < c_i < l$. Then $e$ is a lift of $\varepsilon$, that is, an inverse image of $\varepsilon$ by the canonical surjection $\mathbb{Z}[\Delta] \to \mathbb{F}_l[\Delta]$. Let $\eta_j$, $j = 1, 2, \ldots, d$ be a basis of $k(\zeta)$ as a $k$-module. Let $a(t)$ be a linear form $\sum_{j=1}^{d} t_j \eta_j \in k(t, \zeta)$ over $k(\zeta)$. Then $f(t, X) = F(a(t), X)$ is equal to

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

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

**Proposition 1.1** (Cohen [1]). The polynomial $f(t, X)$ is a $k$-parametric and $C_l$-polynomial.

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

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

$$X^3 - 3(t_1^2 - t_1 t_2 + t_2^2)X + (t_1 + t_2)(t_1^2 - t_1 t_2 + t_2^2) = X^3 - 3N(a)X - \text{Tr}(a)N(a)$$

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

$$f(t, X) = F(a(t), X) = X^5 - 10N(a)X^3 - 5N(a)\text{Tr}(a_1 a_2)X^2 - 5N(a)(\text{Tr}(a_1^2 a_2 a_3) - N(a))X - N(a)\text{Tr}(a_1^2 a_2 a_3^2)$$

where $a = a(t)$, $a_i = \sigma_i(a)$, $N(z) = \prod_{\sigma \in \Delta} \sigma(z)$ and $\text{Tr}(z) = \sum_{\sigma \in \Delta} \sigma(z)$ for $z \in k(t, \zeta)$. 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 \( f(t, X) = F(a(t), X) \) is equal to

\[
F(a(t), X) = X^7 - 21N(a)X^5 - 7N(a)(\text{Tr}(a_1a_2a_3) + 2\text{Tr}(a_1a_2a_4)/3)X^4
- 7N(a)(\text{Tr}(a_1^2a_2^2a_3a_4) + 3\text{Tr}(a_1^2a_2a_3a_4a_5) - 9N(a))X^3
- 7N(a)(2\text{Tr}(a_1^3a_2^3a_3^2a_4^2a_5) + \text{Tr}(a_1^3a_2a_3a_4a_5^2)
+ N(a)(\text{Tr}(a_1a_2a_3) - 2\text{Tr}(a_1a_2a_4)))X^2
- 7N(a)(\text{Tr}(a_1^4a_2^4a_3^3a_4^2a_5^2) - 2\text{Tr}(a_1^3a_2^3a_3a_4a_5)
+ 3\text{Tr}(a_1^3a_2a_3a_4^2a_5) + 4\text{Tr}(a_1^2a_2a_3a_4a_5)
- 9N(a))X
- N(a)(\text{Tr}(a_1^5a_2^5a_3a_4a_5^2) - 7N(a)(\text{Tr}(a_1^3a_2^3a_3^2a_4^2a_5)
- 2\text{Tr}(a_1^3a_2^3a_3a_4^2a_5) + 3\text{Tr}(a_1^3a_2^2a_3^2a_4a_5)
+ \text{Tr}(a_1^3a_2a_3a_4^3a_5^2)
- 2\text{Tr}(a_1^2a_2a_3a_4^2a_5^2) + 2N(a)(\text{Tr}(a_1a_2a_3) - \text{Tr}(a_1a_2a_4)))
\]

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

In this paper we study the arithmetic of the polynomial \( f(t, X) \), 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 \( \text{Spl}(k(t))f(t, X) \) of \( k(t) \) (Proposition 2.1). In the section 3 we introduce a group \( S \) to solve the subfield problem of the generic polynomial \( f(t, X) \) (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).

\section{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 \( f(t, X) \) be the \( C_l \)-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 \( \text{Tr}_H(\zeta^jA) \) of the polynomial \( f(t, X) \). Since \( \text{Spl}(\mathbb{Q}(t))f(t, X) \) is a cyclic extension of \( \mathbb{Q}(t) \) with degree \( l \), there exist rational functions \( \lambda_{ij} \in \mathbb{Q}(t) \) such that \( x_i = \sum_{j=0}^{l-1} \lambda_{ij}x_j^j \).

We define the three \( (l \times l) \)-matrices \( \Lambda \), \( C \) 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.

\textbf{Proposition 2.1.} We have \( \Lambda = CV^{-1} \).

\textit{Proof.} It follows from the definition that \( C = \Lambda V \). Since the zeros \( x_j \) of \( f(t, X) \) 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 \( a(t) = t_1\zeta + t_2\zeta^2 \).
Proposition 2.1 implies that
\[
\Lambda = \begin{bmatrix}
0 & 0 & 1 & 0 \\
2(t_1^2 - t_1 t_2 + t_2^2) & t_1 & 0 & -1 \\
-2(t_1^2 - t_1 t_2 + t_2^2) & t_1 - t_2 & t_1 & 0 \\
t_1 - t_2 & 0 & t_1 & -1 \\
\end{bmatrix}.
\]
This shows that
\[
x_1 = -\frac{1}{t_1 - t_2} x_0^2 - \frac{t_1}{t_1 - t_2} x_0 + \frac{2(t_1^2 - t_1 t_2 + t_2^2)}{t_1 - t_2},
\]
\[
x_2 = \frac{1}{t_1 - t_2} x_0^2 + \frac{t_2}{t_1 - t_2} x_0 - \frac{2(t_1^2 - t_1 t_2 + t_2^2)}{t_1 - t_2}.
\]

§ 3. Group structure

In this section we define a group to solve the subfield problem of the generic polynomial $f(t, X)$. Let us assume that $k = \mathbb{Q}$ and $a(t) = \sum_{j=1}^{l-1} t_j \zeta^j$. Recall that $e = \sum_{i=1}^{l-1} c_i \sigma_i \in \mathbb{Z}[\Delta]$ where $-i c_i \equiv 1 \pmod{l}$ and $0 < c_i < l$. For an integer $i$ with $0 < i < l$ we denote the linear form $\sigma_i(a(t))$ by $a_i(t)$ and the polynomial $e(a_i(t)) \in \mathbb{Q}(\zeta)[t]$ by $g_i(t)$. We denote $(a_i(t))_{i=1}^{l-1}$ by $\mathfrak{a}(t)$ and $(g_i(t))_{i=1}^{l-1}$ by $\mathfrak{g}(t)$. We define a subspace $S$ of $A^{l-1}$ by
\[
S = \{ \mathfrak{s} = (s_1, s_2, \ldots, s_{l-1}) | a_i(s) \neq 0 \text{ for every } i \in \mathbb{Z} \text{ with } 0 < i < l \}.
\]
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
\[
s_j = \sum_{i=1}^{j-1} q_{i} r_{j-i} + \sum_{i=j+1}^{l-1} q_{i} r_{l+j-i} - \sum_{i=1}^{l-1} q_{i} r_{l-i}
\]
with $0 < j < l$. For an integer $i$ with $0 < i < l$ we define a rational function $m_i(t) \in \mathbb{Q}(t)$ by $m_i(t) = \text{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}(t)}((\zeta^{-i} - 1)/a_1(t))/l$, and denote $(m_i(t))_{i=1}^{l-1}$ by $\mathfrak{m}(t)$.

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

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

**Lemma 3.2.** We have $\mathfrak{g}(t) = \mathfrak{a}(\hat{\mathfrak{g}}(t))$. 
Let $K$ be an extension field of $\mathbb{Q}$. For a $K$-valued element $s \in S(K)$ of $S$ let $L_s$ denote the minimal splitting field $\text{Spl}_K f(s, X)$ over $K$ of $f(s, X) \in K[X]$. For a positive integer $n$ and $s \in S$ let $[n](s)$ denote the sum $s + s + \cdots + s$ with $n$ terms.

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

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

$$S = \{(s_1, s_2) \in K^2 | s_1^2 - s_1 s_2 + s_2^2 \neq 0\}$$

$$(q_1, q_2) + S (r_1, r_2) = (q_2 r_2 - q_1 r_2 - q_2 r_1, q_1 r_1 - q_1 r_2 - q_2 r_1),$$

$$\text{id}_S = (-1, -1),$$

$$m(s_1, s_2) = \left(\frac{s_2}{s_1^2 - s_1 s_2 + s_2^2}, \frac{s_1}{s_1^2 - s_1 s_2 + s_2^2}\right),$$

$$\hat{g}(s_1, s_2) = (s_1^3 - s_1^2 s_2 + s_1 s_2^2, s_1^2 s_2 - s_1 s_2^2 + s_2^3).$$

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

**Theorem 4.1.** If $p$ is not equal to $l$ and $s \pmod{p}$ belongs to $S(\mathbb{F}_p)$, then $L_s/K$ is unramified at $p$. In such a case, the Frobenius automorphism $\left(\frac{L_s/K}{p}\right)$ of $p$ in the extension $L_s/K$ is equal to $\tau_1^j$ where $j$ is an integer satisfying

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

**Proof.** The condition $s \pmod{p} \in S(\mathbb{F}_p)$ implies that the additive $\mathfrak{P}$-adic valuation $v_\mathfrak{P}(g_1(s))$ of $g_1(s)$ is equal to 0. It follows from $\mathfrak{P} \nmid l$ that $\mathfrak{P}$ is unramified in $L_s(\zeta)/K(\zeta)$ and so is $p$ in $L_s/K$. For an element $\tau \in \text{Gal}(L_s/K)$ let $\tilde{\tau}$ be the extension
of τ to Gal(L_{s}(ζ)/K) such that τ(ζ) = ζ. It is easily seen that τ_{1}(\sqrt[p]{g_{1}(s)}) = \sqrt[p]{g_{1}(s)} for τ_{1}(x_{i}) = x_{i+1} and τ_{1}(ζ) = ζ. For an element τ ∈ Gal(L_{s}(ζ)/K(ζ)) let τ_{K} denote the image of τ by the natural inclusion map Gal(L_{s}(ζ)/K(ζ)) → Gal(L_{s}(ζ)/K). It is known (cf. Fröhlich–Taylor [3] Theorem 30) that
\left(\frac{L_{s}(ζ)/K}{\mathfrak{p}}\right)^{d_{\mathfrak{P}/\mathfrak{p}}} = \left(\frac{L_{s}(ζ)/K(ζ)}{\mathfrak{p}}\right)_{K}
and
\left(\frac{L_{s}(ζ)/K}{\mathfrak{p}}\right)_{L_{s}} = \left(\frac{L_{s}/K}{\mathfrak{p}}\right).

Now suppose that \left(\frac{L_{s}/K}{\mathfrak{p}}\right) = τ_{1}^{j} for some j ∈ \mathbb{Z}. Then one has that τ_{1}^{jd_{\mathfrak{P}/\mathfrak{p}}} = \left(\frac{L_{s}(ζ)/K(ζ)}{\mathfrak{P}}\right)_{K}L_{s}^{j}
by class field theory, if \left(\frac{L_{s}/K}{\mathfrak{p}}\right) = \tau_{1}^{j_{1}} (mod \mathfrak{P}). The elements \tilde{τ}_{1}|_{L_{s}} and τ_{1} coincide and have order l. This means that jd_{\mathfrak{P}/\mathfrak{p}} = j_{1} (mod l). Thus it holds that
\left(\frac{L_{s}(ζ)/K(ζ)}{\mathfrak{P}}\right)_{K}L_{s}^{j} = \left(\frac{L_{s}/K}{\mathfrak{p}}\right).

By the definition of \hat{\mathfrak{g}}(t) we have
\left[\frac{p^{d_{\mathfrak{P}}}-1}{l}\right] \hat{\mathfrak{g}}(s) = [jd_{\mathfrak{P}/\mathfrak{p}}](1,0,0,...,0)
in S(\mathbb{F}_{\mathfrak{p}}).

Here the element η = (1,0,0,...,0) satisfies a_{i}(η) = ζ^{i}. Note that (p^{d_{\mathfrak{P}}}-1)/l and jd_{\mathfrak{P}/\mathfrak{p}} are integers, and \hat{\mathfrak{g}}(s) and η 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(t, X) over \mathbb{Q} are as follows.

**Proposition 4.2.** Let s = (s_{1}, s_{2},..., s_{l-1}) be an element of S(\mathbb{Q}) such that s_{i} ∈ \mathbb{Z}_{l} and \sum_{i=1}^{l-1}s_{i} ≠ 0 (mod l). Then the extension Sp_{Q}f(s, X) of \mathbb{Q} is unramified at l if and only if it satisfies \sum_{i=1}^{l-1}is_{i} ≡ 0 (mod l).

**Proof.** Let us denote Sp_{Q}f(s, X) by L. The ramification index of l in L/\mathbb{Q} is equal to that of L in L(ζ)/\mathbb{Q}(ζ) where L = (1 - ζ) is the prime ideal of \mathbb{Q}(ζ) above l. Now put \eta_{0} = \sum_{i=1}^{l-1}s_{i}. It follows from the assumption that \eta_{0} ∈ \mathbb{Z}_{l}. There exist integer n_{1} and a positive integer j such that a(s) ≡ n_{0} + n_{1}(1 - ζ)^{j} (mod \mathfrak{L}^{j+1}). One has
\begin{align*}
e & \left(\frac{a(s)}{n_{0}}\right) \equiv \prod_{i=1}^{l-1} \left(1 - \frac{n(1 - ζ^{i})^{j}}{i}\right) \\
& \equiv \prod_{i=1}^{j}(1 - n(1 - ζ)^{i})^{j-1} \\
& \equiv 1 - n(1 - ζ)^{j} \sum_{i=1}^{j-1}i^{j-1} (mod \mathfrak{L}^{j+1})
\end{align*}
where \( n = n_1/n_0 \in \mathbb{Z}_l \cap \mathbb{Q} \). Thus, estimating the sum \( \sum_{i=1}^{(l-1)/2} i^{j-1} \) modulo \( l \), we have

\[
e\left( \frac{a(s)}{n_0} \right) = \begin{cases} 1 + n(1 - \zeta) & (j = 1), \\ 1 & (2 \leq j \leq l - 1) \end{cases} \quad \text{mod} \ L^{j+1}.
\]

If \( j = 1 \) and \( n_1 \not\equiv 0 \pmod{l} \), then \( e(a(s)/n_0) \equiv 1 \pmod{\mathfrak{L}} \) and \( e(a(s)/n_0) \equiv 1 \pmod{\mathfrak{L}^2} \). This means that \( \mathfrak{L} \) ramifies in \( L_s(\zeta)/\mathbb{Q}(\zeta) \). In fact, \( \text{Spl}_\mathbb{Q} F(a(s), X) = \text{Spl}_\mathbb{Q} F(a(s)/n_0, X) \) for \( e(n_0) \in \mathbb{Q}(\zeta)^\times \). When \( j \geq 2 \), we see that \( e(a(s)/n_0) \equiv 1 \pmod{\mathfrak{L}^j} \) by using the above congruence, repeatedly. Thus \( \mathfrak{L} \) does not ramify in \( L_s(\zeta)/\mathbb{Q}(\zeta) \). Note that \( a(s) - n_0 = \sum_{i=1}^{l-1}(\zeta^i - 1)s_i \equiv (\zeta - 1) \sum_{i=1}^{l-1}is_i \pmod{\mathfrak{L}^2} \). 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.

\[\square\]

**§ 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 \( \omega_i \) and simply \( \omega_1 \) by \( \omega \). For an element \( z \in \mathbb{Q}(t, \omega) \) we denote the trace \( \text{Tr}_{\mathbb{Q}(t, \omega)/\mathbb{Q}(t)}(z) \) by \( \text{Tr}_\omega(z) \). The following properties of \( \omega_i \) are easily seen.

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

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

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

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

\[
\pi_i(t) = -\frac{1}{l} \text{Tr}_\omega \left( \omega_i - 2 - \zeta^{-1}a(t) - \zeta \bar{a}(t) \right) a(t) - \bar{a}(t)
\]

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

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

**Proof.** Since \(-\left( (\zeta^{-1}a(t) - \zeta \bar{a}(t)) / (a(t) - \bar{a}(t)) \right) \) belongs to \( \mathbb{Q}(t, \omega) \), Lemma 5.2 implies that \( \sum_{i=1}^{(l-1)/2} \pi_i(t)\omega_i = -(\zeta^{-1}a(t) - \zeta \bar{a}(t))/ (a(t) - \bar{a}(t)) \). Thus we have \( b(\pi(t)) = \zeta + \sum_{i=1}^{(l-1)/2} \pi_i(t)\omega_i = (\zeta - \zeta^{-1})a(t)/(a(t) - \bar{a}(t)) \). \( \square \)
Proposition 5.4. We have $\text{Sp}_{\mathbb{Q}(t)} h(\pi(t), X) = \text{Sp}_{\mathbb{Q}(t)} f(t, X)$.

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

Corollary 5.5. The polynomial $h(u, X)$ is a $\mathbb{Q}$-generic $C_l$-polynomial.

We can see the arithmetic of $h(u, X)$ by that of $f(t, X)$ 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 $C_l$-polynomial over $\mathbb{Q}$ with $(l - 1)/2$ parameters. Smith decreases the number of the parameters by multiplying elements of $\mathbb{Q}(t, \omega)$ as that for our $h(u, X)$.

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


