

# ANNALES MATHÉMATIQUES



## BLAISE PASCAL

TORU KOMATSU

**Generalized Kummer theory and its applications**

Volume 16, n° 1 (2009), p. 127-138.

<[http://ambp.cedram.org/item?id=AMBP\\_2009\\_\\_16\\_1\\_127\\_0](http://ambp.cedram.org/item?id=AMBP_2009__16_1_127_0)>

© Annales mathématiques Blaise Pascal, 2009, tous droits réservés.

L'accès aux articles de la revue « Annales mathématiques Blaise Pascal » (<http://ambp.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://ambp.cedram.org/legal/>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

*Publication éditée par le laboratoire de mathématiques  
de l'université Blaise-Pascal, UMR 6620 du CNRS  
Clermont-Ferrand — France*

**cedram**

*Article mis en ligne dans le cadre du  
Centre de diffusion des revues académiques de mathématiques  
<http://www.cedram.org/>*

# Generalized Kummer theory and its applications

TORU KOMATSU

## Abstract

In this report we study the arithmetic of Rikuna's generic polynomial for the cyclic group of order  $n$  and obtain a generalized Kummer theory. It is useful under the condition that  $\zeta \notin k$  and  $\omega \in k$  where  $\zeta$  is a primitive  $n$ -th root of unity and  $\omega = \zeta + \zeta^{-1}$ . In particular, this result with  $\zeta \in k$  implies the classical Kummer theory. We also present a method for calculating not only the conductor but also the Artin symbols of the cyclic extension which is defined by the Rikuna polynomial.

## 1. Introduction

In this report we study the arithmetic of Rikuna's generic polynomial for the cyclic group of order  $n$  and obtain a generalized Kummer theory. It is useful under the condition that  $\zeta \notin k$  and  $\omega \in k$  where  $\zeta$  is a primitive  $n$ -th root of unity and  $\omega = \zeta + \zeta^{-1}$ . In particular, this result with  $\zeta \in k$  implies the classical Kummer theory. We also present a method for calculating not only the conductor but also the Artin symbols of the cyclic extension which is defined by the Rikuna polynomial. By an arithmetic argument we show that a certain cubic polynomial is not generic (cf. Corollary 3.6).

We first recall notion on the genericity of a polynomial (cf. Jensen-Ledet-Yui [3]). Let  $k$  be a field and  $G$  a finite group. The rational function field  $k(t_1, t_2, \dots, t_m)$  over  $k$  with  $m$  variables  $t_1, t_2, \dots, t_m$  is denoted by  $k(\mathbf{t})$  where  $\mathbf{t} = (t_1, t_2, \dots, t_m)$ . For a polynomial  $F(X) \in K[X]$  over a field  $K$  let us denote by  $\text{Spl}_K F(X)$  the minimal splitting field of  $F(X)$  over  $K$ . We say that a polynomial  $F(\mathbf{t}, X) \in k(\mathbf{t})[X]$  is a  $k$ -regular  $G$ -polynomial or a regular polynomial over  $k$  for  $G$  if the field  $\text{Spl}_{k(\mathbf{t})} F(\mathbf{t}, X)$  is a Galois extension  $L$  of  $k(\mathbf{t})$  with two conditions  $\text{Gal}(L/k(\mathbf{t})) \simeq G$  and  $L \cap \bar{k} = k$  where  $\bar{k}$  is an algebraic closure field of  $k$ . For example, if  $n$  is a positive

---

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

*Keywords:* Generic polynomial, Kummer theory, Artin symbol.

*Math. classification:* 11R20, 12E10, 12G05.

integer greater than 2, then the Kummer polynomial  $X^n - t \in \mathbf{Q}(t)[X]$  is a regular polynomial for the cyclic group  $\mathcal{C}_n$  of order  $n$  not over  $\mathbf{Q}$  but over  $\mathbf{Q}(\zeta_n)$  where  $\zeta_n$  is a primitive  $n$ -th root of unity in  $\overline{\mathbf{Q}}$ . A  $k$ -regular  $G$ -polynomial  $F(t, X) \in k(t)[X]$  is called to be generic over  $k$  if  $F(t, X)$  yields all the Galois  $G$ -extensions containing  $k$ , that is, for every Galois extension  $L/K$  with  $\text{Gal}(L/K) \simeq G$  and  $K \supseteq k$  there exists a  $K$ -specialization  $\mathfrak{s} = (s_1, s_2, \dots, s_m)$ ,  $s_i \in K$  so that  $L = \text{Spl}_K F(\mathfrak{s}, X)$ .

Let  $n$  be an odd number greater than 1 and  $\zeta = \zeta_n$  a primitive  $n$ -th root of unity in  $\overline{\mathbf{Q}}$ . We put  $\omega = \zeta + \zeta^{-1}$  and  $k = \mathbf{Q}(\omega)$ . We define a polynomial  $R_n(t, X)$  by

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

Note that  $R_n(t, X)$  is a polynomial in  $k(t)[X]$ .

**Proposition 1.1** (Rikuna [11]). *The polynomial  $R_n(t, X)$  is generic over the field  $k$  for the group  $\mathcal{C}_n$ .*

*Remark 1.2.* When  $n$  is even and  $K$  does not contain  $\zeta$ , the polynomial  $R_n(t, X)$  is not generic over  $K$  for  $\mathcal{C}_n$  in general (cf. Komatsu [6]). For the case that  $n$  is even, Hashimoto and Rikuna [2] constructed a  $k$ -generic  $\mathcal{C}_n$ -polynomial with two parameters.

In a previous paper [6] we study the arithmetic of the polynomial  $R_n(t, X)$ . Let  $k$  be a field whose characteristic is equal to 0 or prime to  $n$ . Let  $\zeta$  be a primitive  $n$ -th root of unity in  $\overline{k}$  and put  $\omega = \zeta + \zeta^{-1}$ . For a field  $K$  containing  $k(\omega)$  let  $T(K) = \mathbf{P}^1(K) - \{\zeta, \zeta^{-1}\} = K \cup \{\infty\} - \{\zeta, \zeta^{-1}\}$  be a set with composition  $\frac{+}{T}$  such that  $s_1 \frac{+}{T} s_2 = (s_1 s_2 - 1)/(s_1 + s_2 - \omega)$ . Then  $T(K)$  is an algebraic torus of dimension 1 which has a group isomorphism  $\varphi : T \rightarrow \mathbf{G}_m$ ,  $t \mapsto (t - \zeta)/(t - \zeta^{-1})$  over  $K(\zeta)$ . In fact, the composition  $\frac{+}{T}$  is defined as  $s_1 \frac{+}{T} s_2 = \varphi^{-1}(\varphi(s_1)\varphi(s_2))$ . The identity  $0_T$  on  $T$  is equal to  $\infty = \varphi^{-1}(1)$ . The inverse  $\frac{-}{T}s$  of an  $s \in T(K)$  is  $-s + \omega$ . For a positive integer  $m \in \mathbf{Z}$  let  $[m]$  be the multiplication map by  $m$  with respect to  $\frac{+}{T}$ , that is,  $[m]s = s \frac{+}{T} \cdots \frac{+}{T} s$  with  $m$  terms. We denote  $[m]T(K) = \{[m]s | s \in T(K)\}$  and  $T[m] = T(\overline{K})[m] = \{x \in T(\overline{K}) | [m]x = \infty\}$ . Note that  $-1 = \varphi^{-1}(\zeta)$  and  $T[n] = \langle -1 \rangle_T = \{-1, 0, \dots, \omega, \omega + 1, \infty\} \subset T(k(\omega))$ . Let  $\Gamma_K$  be the

absolute Galois group  $\text{Gal}(K^{\text{sep}}/K)$  of  $K$  where  $K^{\text{sep}}$  is the separable closure field of  $K$ . Then we have a descent Kummer theory.

**Proposition 1.3** (Ogawa [10], Komatsu [6]). *There exists a group isomorphism*

$$\delta : T(K)/[n]T(K) \rightarrow \text{Hom}_{\text{cont}}(\Gamma_K, \mathcal{C}_n).$$

We have a relation between the polynomial  $R_n(t, X)$  and the algebraic group  $T$  as follows. For an  $s \in T(K)$  let  $L_s$  be the field  $\text{Spl}_K R_n(s, X)$  and  $[n]^{-1}(s)$  the set  $\{x \in T(\overline{K}) \mid [n]x = s\}$ .

**Lemma 1.4.** *We have  $L_s = K([n]^{-1}(s))$ . In particular, the field  $L_s$  is equal to the fixed field  $(K^{\text{sep}})^{\text{Ker}\delta(s)}$  of  $K^{\text{sep}}$  by the subgroup  $\text{Ker}\delta(s)$  of  $\Gamma_K$ .*

**Corollary 1.5.** *For elements  $s_1$  and  $s_2 \in K$  the equation  $L_{s_1} = L_{s_2}$  holds if and only if  $\langle s_1 \rangle_T = \langle s_2 \rangle_T$  in  $T(K)/[n]T(K)$ .*

*Remark 1.6.* Morton [9] and Chapman [1] essentially gave the composition  $+$  for the case  $n = 3$ . Here  $R_3(t/3, X) = X^3 - tX^2 - (t+3)X - 1$  is known as the simplest cubic polynomial of Shanks type.

## 2. Ramifications and Artin symbols

In this section we recall some results in [6] and [7]. Let  $l$  be an odd prime number and  $\zeta$  a primitive  $l$ -th root of unity in  $\overline{\mathbf{Q}}$ . Let  $K$  be a finite algebraic number field containing  $\mathbf{Q}(\omega)$  where  $\omega = \zeta + \zeta^{-1}$ . We assume that the extension  $K/\mathbf{Q}(\omega)$  is unramified at all the prime ideals of  $K$  above  $l$ . For an  $s \in K$  we denote by  $L_s$  the minimal splitting field  $\text{Spl}_K R_l(s, X)$  of the polynomial  $R_l(s, X)$  over the field  $K$ . For a prime ideal  $\mathfrak{p}$  of  $K$  let  $v_{\mathfrak{p}}$  be a  $\mathfrak{p}$ -adic additive valuation which is normalized so that  $v_{\mathfrak{p}}(K^\times) = \mathbf{Z}$ . For a prime ideal  $\mathfrak{l}$  of  $K$  above  $l$  we define a set  $U_{K,\mathfrak{l}}$  by

$$U_{K,\mathfrak{l}} = \{s \in T(K) \mid v_{\mathfrak{l}}(s - \omega/2) \leq -(l-1)/2 \text{ or } v_{\mathfrak{l}}(s - \omega/2) \geq (l+1)/2\}.$$

For a prime ideal  $\mathfrak{q}$  of  $K$  with  $\mathfrak{q} \nmid l$  the set  $U_{K,\mathfrak{q}}$  is defined to be

$$U_{K,\mathfrak{q}} = \{s \in T(K) \mid v_{\mathfrak{q}}(s^2 - \omega s + 1) \leq 0 \text{ or } v_{\mathfrak{q}}(s^2 - \omega s + 1) \equiv 0 \pmod{l}\}.$$

**Lemma 2.1** (Komatsu [6]). *For an  $s \in K$  the conductor  $\text{cond}(L_s/K)$  of the extension  $L_s/K$  is equal to  $\prod_{\mathfrak{p}} \mathfrak{p}^{\lambda_{\mathfrak{p}}}$  where*

$$\lambda_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid l \text{ and } s \notin U_{K,\mathfrak{p}}, \\ \mathfrak{c}_{\mathfrak{l}}(s) & \text{if } \mathfrak{p} = \mathfrak{l} \mid l \text{ and } s \notin U_{K,\mathfrak{l}}, \\ 0 & \text{otherwise.} \end{cases}$$

Here  $\mathfrak{c}_{\mathfrak{l}}(s)$  is equal to a positive integer  $(l+2)/2 - |v_{\mathfrak{l}}(s - \omega/2) - 1/2|$  for  $s \notin U_{K,\mathfrak{l}}$ .

We denote by  $U_K$  the intersection  $\bigcap_{\mathfrak{p}} U_{K,\mathfrak{p}}$  of the sets  $U_{K,\mathfrak{p}}$  where  $\mathfrak{p}$  runs through all of the prime ideals of  $K$ . In general, one has that  $[l]T(K) \subseteq U_K$ .

**Corollary 2.2.** *Vandiver conjecture for  $\mathbf{Q}(\omega)$  is true, that is, the class number of  $\mathbf{Q}(\omega)$  is not divisible by  $l$  if and only if it satisfies  $[l]T(\mathbf{Q}(\omega)) = U_{\mathbf{Q}(\omega)}$ . In particular, an unramified cyclic extension of  $\mathbf{Q}(\omega)$  with degree  $l$  is obtained as  $\text{Spl}_{\mathbf{Q}(\omega)} R_l(s, X)$  for an  $s \in U_{\mathbf{Q}(\omega)} - [l]T(\mathbf{Q}(\omega))$ .*

Let us assume that  $s \notin [l]T(K)$ , that is,  $L_s/K$  is a cyclic extension of degree  $l$ . Then  $L_s$  is generated over  $K$  by a solution  $x$  of  $R_l(s, X) = 0$ . The Galois group  $\text{Gal}(L_s/K)$  is generated by an element  $\sigma$  such that  $\sigma(x) = x \frac{1}{T}(-1)$ . Note that  $\langle -1 \rangle_T = T[l] \subset T(K)$ . Let  $\mathfrak{p}$  be a prime ideal of  $K$  which is unramified in the extension  $L_s/K$ . We denote by  $\mathbf{F}_{\mathfrak{p}}$  the residue class field  $\mathcal{O}_K/\mathfrak{p}$  and by  $q$  the cardinal number  $\#\mathbf{F}_{\mathfrak{p}}$  of the finite field  $\mathbf{F}_{\mathfrak{p}}$ . Note that  $q \equiv 0$  or  $\pm 1 \pmod{l}$  since  $K$  contains  $\omega$ . We fix a prime ideal  $\mathfrak{P}$  of  $L_s$  above  $\mathfrak{p}$ . Then there exists an element  $\tau \in \text{Gal}(L_s/K)$  such that  $v_{\mathfrak{P}}(\tau(\alpha) - \alpha^q) \geq 1$  for every algebraic integer  $\alpha \in \mathcal{O}_{L_s}$  in  $L_s$ . The element  $\tau$  depends not on the choice of the prime ideal  $\mathfrak{P}$  but only on the prime ideal  $\mathfrak{p}$ . We call  $\tau$  the Artin symbol of  $\mathfrak{p}$  in  $L_s/K$  and denote it by  $\text{Art}_{\mathfrak{p}}(L_s/K)$ . We put  $\mu_{\mathfrak{p}}(s) = v_{\mathfrak{p}}(s^2 - \omega s + 1)$ .

**Theorem 2.3** (Komatsu [7]). *We assume that  $\mathfrak{p} \nmid l$ . If  $\mu_{\mathfrak{p}}(s) < 0$ , then  $\text{Art}_{\mathfrak{p}}(L_s/K) = \text{id}$ , that is,  $\mathfrak{p}$  splits completely in  $L_s/K$ . For the case  $\mu_{\mathfrak{p}}(s) = 0$ , we have  $\text{Art}_{\mathfrak{p}}(L_s/K) = \sigma^i$  where  $i \in \mathbf{Z}$  is an integer such that  $[i](-1) = [(\pm q - 1)/l]s$  in  $T(\mathbf{F}_{\mathfrak{p}})$  provided  $q \equiv \pm 1 \pmod{l}$ , respectively. When  $\mu_{\mathfrak{p}}(s) > 0$  and  $\mu_{\mathfrak{p}}(s) \not\equiv 0 \pmod{l}$ , the extension  $L_s/K$  is totally ramified at  $\mathfrak{p}$ .*

Theorem 2.3 does not deal with an exceptional case that  $\mu_{\mathfrak{p}}(s) > 0$  and  $\mu_{\mathfrak{p}}(s) \equiv 0 \pmod{l}$ , that is,  $\mu_{\mathfrak{p}}(s) = jl$  for a positive integer  $j \in \mathbf{Z}$ . In the

following we may reduce the exceptional case to the case  $\mu_{\mathfrak{p}}(s) \leq 0$ . For a number  $s_0 \in K$  with  $v_{\mathfrak{p}}(s - s_0) = j$  we put  $s_1 = s \frac{[l]}{T} s_0 \in K$ .

**Lemma 2.4.** *We have  $L_s = L_{s_1}$  and  $\mu_{\mathfrak{p}}(s_1) \leq 0$ .*

*Proof.* Corollary 1.5 shows that  $L_s = L_{s_1}$ . Let  $\tilde{\mathfrak{p}}$  be a prime ideal of  $K(\zeta)$  above  $\mathfrak{p}$ . Then one has that  $(v_{\tilde{\mathfrak{p}}}(s - \zeta), v_{\tilde{\mathfrak{p}}}(s - \zeta^{-1})) = (jl, 0)$  or  $(0, jl)$  since  $\tilde{\mathfrak{p}} \nmid l$ . When  $(v_{\tilde{\mathfrak{p}}}(s - \zeta^{\pm 1}), v_{\tilde{\mathfrak{p}}}(s - \zeta^{\mp 1})) = (jl, 0)$ , we have  $(v_{\tilde{\mathfrak{p}}}(s_0 - \zeta^{\pm 1}), v_{\tilde{\mathfrak{p}}}(s_0 - \zeta^{\mp 1})) = (j, 0)$ , respectively. It follows from  $s_1 = s \frac{[l]}{T} s_0$  that

$$\frac{s_1 - \zeta}{s_1 - \zeta^{-1}} = \frac{s - \zeta}{s - \zeta^{-1}} \left( \frac{s_0 - \zeta}{s_0 - \zeta^{-1}} \right)^{-l}.$$

This implies that  $v_{\tilde{\mathfrak{p}}}((s_1 - \zeta)/(s_1 - \zeta^{-1})) = 0$  and  $v_{\tilde{\mathfrak{p}}}(s_1 - \zeta^{\pm 1}) \leq 0$ . Thus we have  $\mu_{\mathfrak{p}}(s_1) = v_{\tilde{\mathfrak{p}}}((s_1 - \zeta)(s_1 - \zeta^{-1})) \leq 0$ .  $\square$

**Proposition 2.5** (Komatsu [7]). *We assume  $(l, K, \mathfrak{p}) = (3, \mathbf{Q}, 3\mathbf{Z})$ . For an  $s \in \mathbf{Q}$  the decomposition of the prime ideal  $3\mathbf{Z}$  in the extension  $L_s/\mathbf{Q}$  is as follows:*

- (i) *the prime  $3\mathbf{Z}$  ramifies in  $L_s/\mathbf{Q}$  if and only if  $v_3(s + 1/2) \in \{0, 1\}$ .*
- (ii) *the prime  $3\mathbf{Z}$  splits completely in  $L_s/\mathbf{Q}$  if and only if  $v_3(s + 1/2) \notin \{-1, 0, 1, 2\}$ .*
- (iii) *the ideal  $3\mathbf{Z}$  remains prime in  $L_s/\mathbf{Q}$  if and only if  $v_3(s + 1/2) \in \{-1, 2\}$ . When  $v_3(s + 1/2) = -1$  and  $3s \equiv \mp 1 \pmod{3}$ , we have  $\text{Art}_{3\mathbf{Z}}(L_s/\mathbf{Q}) = \sigma^{\pm 1}$ , respectively. For the case  $v_3(s + 1/2) = 2$  and  $(s + 1/2)/9 \equiv \pm 1 \pmod{3}$ , it satisfies  $\text{Art}_{3\mathbf{Z}}(L_s/\mathbf{Q}) = \sigma^{\pm 1}$ , respectively.*

Let  $f_0(t, X)$  be the cubic polynomial  $R_3(t, X) = X^3 - 3tX^2 - (3t + 3)X - 1$ . For a rational number  $s \in \mathbf{Q}$  let  $L_s$  denote the minimal splitting field  $\text{Spl}_{\mathbf{Q}} f_0(s, X)$  of  $f_0(s, X)$  over  $\mathbf{Q}$ . Now assume that  $s \notin [3]T(\mathbf{Q})$ , that is,  $L_s$  is a cyclic cubic extension of  $\mathbf{Q}$ . Then it holds that  $L_s = \mathbf{Q}(x)$  for a solution  $x \in \overline{\mathbf{Q}}$  of  $R_3(s, X) = 0$ . Let  $\sigma$  be a generator of  $\text{Gal}(L_s/\mathbf{Q})$  such that  $\sigma(x) = x \frac{[-1]}{T} = (-x - 1)/x$ . The following table shows the Artin

symbols  $\text{Art}_p(L_s/\mathbf{Q})$  for prime numbers  $p$  with  $2 \leq p \leq 19$  and  $p \neq 3$ .

$p$	$\sigma^0$ split	$\sigma^1$ inert	$\sigma^2$ inert	ram. or bl.up
2	$\infty$	0	1	–
5	$\infty, 2$	1, 4	0, 3	–
7	$\infty, 3$	0, 5	1, 6	2, 4
11	$\infty, 2, 5, 8$	0, 6, 7, 9	1, 3, 4, 10	–
13	$\infty, 4, 6, 8$	1, 2, 7, 12	0, 5, 10, 11	3, 9
17	$\infty, 0, 1, 8, 15, 16$	2, 6, 7, 11, 12, 13	3, 4, 5, 9, 10, 14	–
19	$\infty, 0, 1, 9, 17, 18$	4, 10, 12, 13, 15, 16	2, 3, 5, 6, 8, 14	7, 11

The number  $m$  at  $p$ -row in the table above means that  $s$  is a  $p$ -adic integer with  $s \equiv m \pmod{p}$ . For example, if  $s \in \mathbf{Q}$  satisfies that  $v_5(s) \geq 0$  and  $s \equiv 1 \pmod{5}$ , then the ideal  $5\mathbf{Z}$  remains prime in  $L_s/\mathbf{Q}$  and the Artin symbol  $\text{Art}_{5\mathbf{Z}}(L_s/\mathbf{Q})$  is equal to  $\sigma^1 = \sigma$ . The symbol  $\infty$  represents that  $v_p(s)$  is negative, i.e., the image of  $s$  by the reduction map  $T(\mathbf{Q}) \rightarrow T(\mathbf{F}_p)$ ,  $s \mapsto s \pmod{p}$  is equal to  $\infty$ . On the column of “ram. or bl.up”, it holds that  $\mu_p(s) = v_p(s^2 + s + 1) \geq 1$ . If  $\mu_p(s)$  is not divisible by 3, then  $p$  ramifies in  $L_s/\mathbf{Q}$ . When  $\mu_p(s) \equiv 0 \pmod{3}$ , one can blow-up  $s$  to a new  $s_1 \in \mathbf{Q}$  such that  $L_s = L_{s_1}$  and  $\mu_p(s_1) \leq 0$ . In fact, for a number  $s_0 \in \mathbf{Q}$  with  $v_p(s - s_0) = \mu_p(s)/3$  we put  $s_1 = s - \underset{T}{[3]}s_0 \in \mathbf{Q}$ . Then we have  $L_s = L_{s_1}$  and  $\mu_p(s_1) \leq 0$ . The decomposition type of  $p$  in  $L_s/\mathbf{Q}$  coincides with that in  $L_{s_1}/\mathbf{Q}$ , which is determined completely by the data that  $s_1$  belongs to the columns of “split” or “inert”. In particular,  $p$  is unramified in  $L_s/\mathbf{Q}$ . The symbol – at the column of ram. or bl.-up is denoted for the fact that  $p \equiv 2 \pmod{3}$  cannot ramify in any cyclic cubic fields due to class field theory. Indeed, it satisfies  $\mu_p(s) \leq 0$  provided  $p \equiv 2 \pmod{3}$ . The table for  $p = 3$  is as follows.

$v_3(s)$	$\sigma^0$ split	$\sigma^1$ inert	$\sigma^2$ inert	ram.
$\geq 0$	$s \equiv 13 \pmod{27}$	$s \equiv 22 \pmod{27}$	$s \equiv 4 \pmod{27}$	$s \not\equiv 4 \pmod{9}$
$-1$	$\emptyset$	$3s \equiv 2 \pmod{3}$	$3s \equiv 1 \pmod{3}$	$\emptyset$
$\leq -2$	all cases	$\emptyset$	$\emptyset$	$\emptyset$

For example, if  $s$  is a 3-adic integer with  $s \not\equiv 4 \pmod{9}$ , then  $3\mathbf{Z}$  ramifies in  $L_s/\mathbf{Q}$ . When  $v_3(s) \leq -2$ , the prime ideal  $3\mathbf{Z}$  splits completely in  $L_s/\mathbf{Q}$ .

### 3. Numerical examples of cubic polynomials

In this section we study the Artin symbols in the cyclic cubic fields obtained by some cubic polynomials. Let  $\zeta$  be a primitive 3rd root of unity in  $\overline{\mathbf{Q}}$ . Let  $K$  be a field containing  $\mathbf{Q}$ . Let  $f(X)$  be a cubic polynomial over  $K$  of the form  $f(X) = X^3 + a_1X^2 + a_2X + a_3$  whose discriminant is equal to a non-zero square  $\delta^2$  for  $\delta \in K^\times$ . Let  $b_2$  and  $b_3$  be elements in  $K$  such that  $g(X) = f(X - a_1/3) = X^3 + b_2X + b_3$ . One has that  $b_2 = -a_1^2/3 + a_2$  and  $b_3 = 2a_1^3/27 - a_1a_2/3 + a_3$ . Then it holds that

$$\delta^2 = \text{disc}_X f(X) = a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2 = -4b_2^3 - 27b_3^2.$$

When  $b_2 \neq 0$ , we define the invariant  $c \in K$  of the polynomial  $f(X)$  by  $c = -(9b_3 + \delta)/(2\delta)$ . The invariant is determined up to  $\frac{-}{T}$ , that is,  $c$  or  $-c-1$  due to the choice of the signature of the square root  $\delta$  of the discriminant  $\text{disc}_X f(X)$ . If  $b_2 = 0$  and  $b_3 \neq -1$ , then the invariant  $c$  is defined to be  $\varphi^{-1}(-b_3) = (\zeta^{-1}b_3 + \zeta)/(b_3 + 1)$ . For the case  $(b_2, b_3) = (0, -1)$  we set  $c = \zeta$ . Let  $f_0(t, X)$  be the cubic polynomial  $R_3(t, X) = X^3 - 3tX^2 - (3t + 3)X - 1$ .

**Lemma 3.1.** *We have  $\text{Spl}_K f(X) = \text{Spl}_K f_0(c, X)$ .*

*Proof.* When  $b_2 \neq 0$ , it is seen that

$$\begin{aligned} f_0(c, X + c) &= X^3 - \frac{9(27b_3^2 + d^2)}{4\delta^2}X + \frac{27b_3(27b_3^2 + \delta^2)}{4\delta^3} \\ &= X^3 + (9b_3^3/\delta^2)X - 27b_3^3b_3/\delta^3 \\ &= g(X/\gamma)\gamma^3 \end{aligned}$$

where  $\gamma = -3b_2/\delta \in K^\times$ . If  $b_2 = 0$ , then  $\delta^2 = -27b_3^2$  and  $\zeta \in K$ . This implies that  $\varphi^{-1}(-b_3) \in K$  and  $\text{Spl}_K(X^3 + b_3) = \text{Spl}_K f_0(\varphi^{-1}(-b_3), X)$  provided  $b_3 \neq -1$ . For the case of  $(b_2, b_3) = (0, -1)$  it holds that  $\text{Spl}_K f(X) = K = \text{Spl}_K f_0(\zeta, X)$  since  $f(X) = (X - 1)(X - \zeta)(X - \zeta^2)$  and  $f_0(\zeta, X) = (X - \zeta)^3$ .  $\square$

Let us start with  $f(X) = X^3 - 3tX^2 - (3t + 3)X - 1$ . Here it satisfies that  $(a_1, a_2, a_3) = (-3t, -(3t + 3), -1)$  and  $(b_2, b_3) = (-3(t^2 + t + 1), -(2t + 1)(t^2 + t + 1))$ . One has that  $\text{disc}_X f(X) = 3^4(t^2 + t + 1)^2$ . If  $\delta = 3^2(t^2 + t + 1)$ , then  $c = t$  and  $f_0(t, X) = X^3 - 3tX^2 - (3t + 3)X - 1$ , which is the same as the starting one. Lecocheux [8] gave a cubic polynomial

$$f_1(t, X) = X^3 - (t^3 - 2t^2 + 3t - 3)X^2 - t^2X - 1$$



and Kishi [4] constructed cubic polynomials

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

It is calculated that the discriminants  $\text{disc}f_i(t, X)$  of the polynomials  $f_i(t, X)$  are

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

Let  $c_i(t)$  be rational functions in  $\mathbf{Q}(t)$  such that

$$\begin{aligned} c_1(t) &= \frac{t(t^4 - 3t^3 + 6t^2 - 8t + 6)}{3(t - 1)}, \\ c_2(t) &= -\frac{9t^4 - 18t^3 + 18t^2 - 8t + 1}{2t - 1}, \\ c_3(t) &= \frac{t(t^8 + 2t^7 + 9t^6 + 11t^5 + 25t^4 + 18t^3 + 25t^2 + 8t + 9)}{3(t^2 + 1)}, \\ c_4(t) &= -\frac{t(t^{13} + 3t^{11} - 5t^{10} + 6t^9 - 12t^8 + 17t^7 - 18t^6 + 24t^5 \\ &\quad - 23t^4 + 21t^3 - 15t^2 + 11t - 6)}{(3(t^3 + t - 1))}. \end{aligned}$$

**Lemma 3.2.** *We have  $\text{Spl}_{\mathbf{Q}(t)}f_i(t, X) = \text{Spl}_{\mathbf{Q}(t)}f_0(c_i(t), X)$  for  $i = 1, 2, 3$  and 4.*

*Proof.* The equations of the assertion follow from Lemma 3.1 and the algorithm for computing the invariants  $c = c_i(t)$  of  $f_i(t, X)$ , respectively. Indeed, the square roots  $\delta_i(t)$  of the discriminants  $\text{disc}_X f_i(t, X)$  for the computations are

$$\begin{aligned} \delta_1(t) &= (t - 1)(t^2 + 3)(t^2 - 3t + 3), \\ \delta_2(t) &= 3^3(2t - 1)(t^2 - t + 1), \\ \delta_3(t) &= (t^2 + 1)(t^2 + 3)(t^4 + t^3 + 4t^2 + 3), \\ \delta_4(t) &= (t^2 - t + 1)(t^3 + t - 1)(t^4 - t^3 + t^2 - 3t + 3) \\ &\quad \times (t^4 + 2t^3 + 4t^2 + 3t + 3). \end{aligned}$$

□

GENERALIZED KUMMER THEORY

It is seen that  $c_i(t)^2 + c_i(t) + 1$  have the cubes of polynomials  $\eta_i(t)$  as factors where  $\eta_1(t) = t^2 - t + 1$ ,  $\eta_2(t) = 3t^2 - 3t + 1$ ,  $\eta_3(t) = t^4 + t^3 + 3t^2 + t + 1$  and  $\eta_4(t) = t^6 + t^4 - 2t^3 + t^2 - t + 1$ , respectively. As the blow-up argument before Lemma 2.4 one may think that there exist rational functions  $\tilde{c}_i(t)$  more “suitable” than  $c_i(t)$  such that  $\text{Spl}_{\mathbf{Q}(t)} f_0(\tilde{c}_i(t), X) = \text{Spl}_{\mathbf{Q}(t)} f_0(c_i(t), X)$ . We define  $\varepsilon_1(t) = -t$ ,  $\varepsilon_2(t) = -3t + 1$ ,  $\varepsilon_3(t) = -(t^2 + t + 1)/t$  and  $\varepsilon_4(t) = -(t^3 + t - 1)/t$ . Indeed, it holds that  $\eta_i(t) \mid (c_i(t) - \varepsilon_i(t))$  for  $i = 1, 2, 3$  and 4. Now put  $\tilde{c}_i(t) = c_i(t) - \frac{[3]\varepsilon_i(t)}{T}$ , respectively. The direct computation implies

**Lemma 3.3.** *We have*

$$\begin{aligned} \tilde{c}_1(t) &= \frac{t(t-3)}{3(t-1)}, & \tilde{c}_1(t)^2 + \tilde{c}_1(t) + 1 &= \frac{(t^2+3)(t^2-3t+3)}{3^2(t-1)^2}, \\ \tilde{c}_2(t) &= t-1, & \tilde{c}_2(t)^2 + \tilde{c}_2(t) + 1 &= t^2 - t + 1, \\ \tilde{c}_3(t) &= \frac{t^2(t-1)}{3(t^2+1)}, & \tilde{c}_3(t)^2 + \tilde{c}_3(t) + 1 &= \frac{(t^2+3)(t^4+t^3+4t^2+3)}{3^2(t^2+1)^2}, \\ \tilde{c}_4(t) &= \frac{t(t+1)(t^3-t^2+t-3)}{3(t^3+t-1)}, \\ \tilde{c}_4(t)^2 + \tilde{c}_4(t) + 1 &= \frac{(t^2-t+1)(t^4-t^3+t^2-3t+3)}{\times(t^4+2t^3+4t^2+3t+3)/(3^2(t^3+t-1)^2)}. \end{aligned}$$

For the equation

$$\text{Spl}_{\mathbf{Q}(t)} f_2(t, X) = \text{Spl}_{\mathbf{Q}(t)} f_0(\tilde{c}_2(t), x) = \text{Spl}_{\mathbf{Q}(t)} f_0(t-1, X),$$

we omit the following argument for the case of  $f_2(t, X)$ . Let us fix  $i = 1, 3$  and 4. For a rational number  $s \in \mathbf{Q}$  we denote by  $M_s$  the field  $L_{\tilde{c}_i(s)} = \text{Spl}_{\mathbf{Q}} f_0(\tilde{c}_i(s), X) = \text{Spl}_{\mathbf{Q}} f_i(s, X)$ . Assume that  $\tilde{c}_i(s) \notin [3]T(\mathbf{Q})$ . Let  $x$  be a solution of  $f_0(\tilde{c}_i(s), X) = 0$  and  $\sigma$  a generator of  $\text{Gal}(M_s/\mathbf{Q})$  such that  $\sigma(x) = x + \frac{(-1)}{T} = (-x-1)/x$ . The decomposition types and the Artin symbols  $\text{Art}_p(M_s/\mathbf{Q})$  in  $M_s/\mathbf{Q}$  of prime numbers  $p \leq 19$  are as follows.

T. KOMATSU

For the polynomial  $f_0(\tilde{c}_1(t), X)$  we have

$p$	$\sigma^0$ split	$\sigma^1$ inert	$\sigma^2$ inert	ram. or bl.up
2	$\infty, 1(4)$	$0(2), 3(4)$	$\emptyset$	–
3	$\infty, 1$	$\emptyset$	2	$0 \Rightarrow$ ram.
5	$\infty, 1$	2, 4	0, 3	–
7	$\infty, 1$	0, 3	$\emptyset$	2, 4, 5, 6
11	$\infty, 1, 9$	0, 3, 4	2, 5, 6, 7, 8, 10	–
13	$\infty, 1, 2, 12$	4, 9	0, 3, 8, 10	5, 6, 7, 11
17	$\infty, 0, 1, 3, 4, 5, 6, 9$	7, 10, 11, 12, 14	2, 8, 13, 15, 16	–
19	$\infty, 0, 1, 3, 8, 17$	2, 5, 7, 10, 18	6, 11, 12, 14, 16	4, 9, 13, 15

The integer  $m$  at the  $p$ -row in the table above implies that  $s$  is a  $p$ -adic integer with  $s \equiv m \pmod{p}$ . The symbol  $\infty$  at the  $p$ -row means that  $v_p(s)$  is negative. The notation  $m(p^j)$  represents that  $s$  is a  $p$ -adic integer with  $s \equiv m \pmod{p^j}$ . For the polynomial  $f_0(\tilde{c}_3(t), X)$  we have

$p$	$\sigma^0$ split	$\sigma^1$ inert	$\sigma^2$ inert	ram. or bl.up
2	$\infty$	$0(2), 1(4)$	$3(4)$	–
3	$\infty, 43(81)$	$2(3), 16(81)$	$70(81)$	o.w. <sup>1</sup> $\Rightarrow$ ram.
5	$\infty, 2, 3$	$\emptyset$	0, 1, 4	–
7	$\infty, 4$	0, 1	$\emptyset$	2, 3, 5, 6
11	$\infty, 3, 9$	0, 1, 7, 10	2, 4, 5, 6, 8	–
13	$\infty, 4, 5, 8, 10, 12$	2, 9, 11	0, 1, 3	6, 7
17	$\infty, 0, 1, 2, 4, 13$	9, 10, 11, 12, 15, 16	3, 5, 6, 7, 8, 14	–
19	$\infty, 0, 1, 2, 9, 14$	3, 5, 6, 10	$\begin{cases} 7, 8, 11, 12, \\ 13, 16, 17, 18 \end{cases}$	4, 15

Here the “o.w.<sup>1</sup>” in the table means the otherwise case, which is equivalent to the condition that  $0(3)$ ,  $1(9)$ ,  $4(9)$ ,  $7(27)$  and  $25(27)$ . In such a case, the extension  $M_s/\mathbf{Q}$  is ramified at 3. For the polynomial  $f_0(\tilde{c}_4(t), X)$  we

GENERALIZED KUMMER THEORY

have

$p$	$\sigma^0$ split	$\sigma^1$ inert	$\sigma^2$ inert	ram. or bl.up
2	$\infty$	0, 1	$\emptyset$	–
3	$\infty, 20(27), 14(81)$	1(3), 2(27), 41(81)	11(27), 68(81)	o.w. <sup>2</sup> $\Rightarrow$ ram.
5	$\infty, 1$	2	0, 3, 4	–
7	$\infty, 2$	0, 4, 6	1	3, 5
11	$\infty, 2, 8, 9$	0, 1, 7, 10	3, 4, 5, 6	–
13	$\infty, 6$	5	0, 2, 3, 7, 12	1, 4, 8, 9, 10, 11
17	$\left\{ \begin{array}{l} \infty, 0, 5, 6, 8, \\ 12, 13, 15, 16 \end{array} \right.$	2, 3, 4, 7, 9, 11, 14	1, 10	–
19	$\infty, 0, 4, 14, 18$	9, 10, 13, 15, 17	1, 6, 7, 11	2, 3, 5, 8, 12, 16

The “o.w.<sup>2</sup>” in the table means the otherwise case, which is equivalent to the condition that 0(3), 8(9), 5(27) and 23(27). In such a case,  $M_s/\mathbf{Q}$  is ramified at 3.

**Theorem 3.4.** *The family  $\{\text{Spl}_{\mathbf{Q}}f_1(s, X) \mid s \in \mathbf{Q}\}$  does not contain any cyclic cubic fields  $E$  which are unramified at two prime numbers 2 and 3 with  $\text{Art}_2(E/\mathbf{Q}) = \text{Art}_3(E/\mathbf{Q}) \neq \text{id}$ .*

Let  $E_{13}$  and  $E_{19}$  be cyclic cubic fields with conductor 13 and 19, respectively.

**Lemma 3.5.** *For  $i = 13$  and 19 we have  $\text{Art}_2(E_i/\mathbf{Q}) = \text{Art}_3(E_i/\mathbf{Q}) \neq \text{id}$ , respectively.*

**Corollary 3.6.** *The polynomials  $f_1(t, X)$  is not generic over  $\mathbf{Q}$  for  $\mathcal{C}_3$ .*

*Remark 3.7.* By a geometric approach it is already shown that the polynomials  $f_1(t, X)$ ,  $f_3(t, X)$  and  $f_4(t, X)$  are not generic for  $\mathcal{C}_3$  over any finite algebraic number fields (cf. [5]).

*Remark 3.8.* There are symbols  $\emptyset$  at 7-rows in the tables for  $f_0(\tilde{c}_1(t), X)$  and  $f_0(\tilde{c}_3(t), X)$ , respectively. However, the case of  $\text{Art}_7(M_s/\mathbf{Q}) = \sigma^2$  occurs because of some blowing-up cases.

## References

- [1] R. J. CHAPMAN – Automorphism polynomials in cyclic cubic extensions, *J. Number Theory* **61** (1996), p. 283–291.

T. KOMATSU

- [2] K. HASHIMOTO et Y. RIKUNA – On generic families of cyclic polynomials with even degree, *Manuscripta Math.* **107** (2002), p. 283–288.
- [3] C. U. JENSEN, A. LEDET et N. YUI – *Generic polynomials*, Cambridge University Press, Cambridge, 2002.
- [4] Y. KISHI – A family of cyclic cubic polynomials whose roots are systems of fundamental units, *J. Number Theory* **102** (2003), p. 90–106.
- [5] T. KOMATSU – Potentially generic polynomial, To be submitted.
- [6] ———, Arithmetic of Rikuna’s generic cyclic polynomial and generalization of Kummer theory, *Manuscripta Math.* **114** (2004), p. 265–279.
- [7] ———, Cyclic cubic field with explicit Artin symbols, *Tokyo Journal of Mathematics* **30** (2007), p. 169–178.
- [8] O. LECACHEUX – Units in number fields and elliptic curves, *Advances in number theory*, Oxford Univ. Press, New York, 1993, p. 293–301.
- [9] P. MORTON – Characterizing cyclic cubic extensions by automorphism polynomials, *J. Number Theory* **49** (1994), p. 183–208.
- [10] H. OGAWA – Quadratic reduction of multiplicative group and its applications, *Surikaisekikenkyusho Kokyuroku* **1324** (2003), p. 217–224.
- [11] Y. RIKUNA – On simple families of cyclic polynomials, *Proc. Amer. Math. Soc.* **130** (2002), p. 2215–2218.

TORU KOMATSU  
Faculty of Mathematics  
Kyushu University  
6-10-1 Hakozaki Higashiku  
Fukuoka, 812-8581  
Japan  
trkomatu@math.kyushu-u.ac.jp