Cyclic cubic field with explicit Artin symbols

Komatsu, Toru
Faculty of Mathematics, Kyushu University

出版情報：MHF Preprint Series. 2005-28, 2005-07-28. 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

Cyclic cubic field with explicit Artin symbols

T. Komatsu

MHF 2005-28

(Received July 28, 2005)

Faculty of Mathematics
Kyushu University
Fukuoka, JAPAN

Cyclic cubic field with explicit Artin symbols

Toru KOMATSU

Abstract. In this paper we present a set $\mathcal{T}_f^+$ of rational numbers $s \in \mathbb{Q}$ such that the minimal splitting fields L_s of $X^3 - 3sX^2 - (3s+3)X - 1$ are cyclic cubic fields with a given conductor f. The set $\mathcal{T}_f^+$ has exactly one s for each field L of conductor f. The Weil's height of every number $s \in \mathcal{T}_f^+$ is minimal among all of the rational numbers $s \in \mathbb{Q}$ such that $L_s = L$. If a cyclic cubic field L of conductor f is given, then we can choose the number $s \in S$ corresponding to L by sequencing the explicit Artin symbols.

§ 0. Introduction

Recently many mathematicians construct generic polynomials and expect to apply the polynomials to the case of algebraic number fields. In this paper we make use of a generic cyclic cubic polynomial $F(t, X) = X^3 - 3tX^2 - (3t+3)X - 1$, which is well-known as the simplest cubic polynomial of Shanks type (cf. Shanks [**14**], Serre [**13**]). Hashimoto-Miyake [**4**] and Rikuna [**12**] generalize the polynomial $F(t, X)$ to the cases of general degree, and the author [**6**] studies the arithmetic properties of the general degree cases. For a rational number $s \in \mathbb{Q}$ let L_s be the minimal splitting field of $F(s, X)$ over $\mathbb{Q}$. We give a method for making a rational number $s \in \mathbb{Q}$ such that L_s is equal to a given cyclic cubic field L. Let $f = f_L$ be the conductor of L and $\mathcal{P}_f$ the set of prime divisors of f. For a prime number p with $p \equiv 1 \pmod 3$ we denote a rational number $a_p/b_p \in \mathbb{Q}$ by c_p where (a_p, b_p) is a unique pair in the set $\{(a, b) \in \mathbb{Z} \times \mathbb{Z} | a^2 + ab + b^2 = p,\ b \equiv 0 \pmod 3,$ $b > 0$ and $a/b \geq -1/2\}$. Put $c_3 = 0$. In a previous paper [**6**] we defined an algebraic torus $T(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ of dimension 1 with composition $+_T$ such that $s_1 +_T s_2 = (s_1 s_2 - 1)/(s_1 + s_2 + 1)$. Note that the identity 0_T on T is ∞, and the inverse $-_T s$ of s is equal to $-s - 1$. Let $\mathcal{T}_f$ be the subset of $T(\mathbb{Q})$ consisting of elements of the form $\Sigma_T [m_p] c_p$ where p runs through all of the prime divisors of f and $m_p \in \{\pm 1\}$. Now define a subset $\mathcal{T}_f^+$ of $\mathcal{T}_f$ such that $\mathcal{T}_f^+ = \{s \in \mathcal{T}_f | s \geq -1/2\}$. Let $\mathcal{L}_f$ be the family of cyclic cubic fields with conductor f.

Theorem 0.1. *There exists a one-to-one correspondence* $R_{F,\mathbb{Q}} : \mathcal{T}_f^+ \to \mathcal{L}_f$, $s \mapsto L_s$.

Let c_L denote the rational number $s \in \mathcal{T}_f^+$ such that $R_{F,\mathbb{Q}}(s) = L$.

Proposition 0.2. *The Weil's height of the number* c_L *is minimal among all of the rational numbers* $s \in \mathbb{Q}$ *satisfying* $L_s = L$.

REMARK 0.3. The composition $+_T$ is essentially given by Morton [**9**] and Chapman [**1**] for the cubic case. The author [**6**] extends the composition for the cases of general degree by using the Rikuna's cyclic polynomial.

Theorem 0.1 implies that there exists exactly one $s \in \mathbb{Q}$ in $\mathcal{T}_f^+$ for the given cyclic cubic field L. To determine the number s in $\mathcal{T}_f^+$ corresponding L we calculate the Artin symbols. Now assume that $L_s/\mathbb{Q}$ is cubic for a rational number $s \in \mathbb{Q}$. Let σ be a generator of $\mathrm{Gal}(L_s/\mathbb{Q})$ such that $\sigma(x) = (-x-1)/x$ for $x \in L_s$ with $F(s,x) = 0$. Let (L_s/p) be the Artin symbol of a prime number p in $L_s/\mathbb{Q}$. We define $\mu_p(s) = v_p(s^2+s+1)$ where v_p is the normalized p-adic additive valuation.

Theorem 0.4. *Assume that $p \neq 3$. If $\mu_p(s) < 0$, then $(L_s/p) = \mathrm{id}$, that is, p splits completely in $L_s/\mathbb{Q}$. For the case $\mu_p(s) = 0$, we have $(L_s/p) = \sigma^i$ where $i \in \mathbb{Z}$ is an integer such that $[i](-1) = [(\pm p-1)/3]s$ in $T(\mathbb{F}_p)$ provided $p \equiv \pm 1 \pmod 3$, respectively. When $\mu_p(s) > 0$ and $\mu_p(s) \not\equiv 0 \pmod 3$, $L_s/\mathbb{Q}$ is totally ramified at p.*

REMARK 0.5. The Artin symbol of $p = 3$ is also calculated (see Proposition 3.3). By using Theorem 0.4 we can calculate (L_s/p) for $s \in \mathcal{T}_f$ and $p \neq 3$. One can extend Theorem 0.4 for the general degree cases.

In §1 we recall the descent Kummer theory described in [**6**]. In §2 we construct a set of rational numbers which correspond to cyclic cubic fields with a given conductor. In §3 we present a method for calculating the explicit Artin symbols. In §4 we have a remark on generators for the ring of integers of the cyclic cubic field L_s as $\mathbb{Z}$-module. In §5 we exhibit some numerical examples.

§ 1. Preparation

We recall some results in the paper [**6**]. Let $T(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ be an algebraic torus of dimension 1 with composition $+_T$ such that $s_1 +_T s_2 = (s_1 s_2 - 1)/(s_1 + s_2 + 1)$. In fact, there exists a group isomorphism $\varphi : T \to \mathbb{G}_m$, $t \mapsto (t-\zeta)/(t-\zeta^{-1})$ over $\mathbb{Q}(\zeta)$ where ζ is a primitive 3rd root of unity. The composition $+_T$ is defined as $s_1 +_T s_2 = \varphi^{-1}(\varphi(s_1)\varphi(s_2))$. The identity 0_T on T is equal to $\infty = \varphi^{-1}(1)$. For a positive integer $m \in \mathbb{Z}$ let $[m]$ be the multiplication map by m with respect to $+_T$, that is, $[m]t = t +_T \cdots +_T t$ with m terms. We denote $[m]T(\mathbb{Q}) = \{[m]s | s \in T(\mathbb{Q})\}$ and $T[m] = T(\overline{\mathbb{Q}})[m] = \{x \in T(\overline{\mathbb{Q}}) | [m]x = \infty\}$. Note that $T[3] = \langle -1 \rangle_T = \{\infty, -1, 0\} \subset T(\mathbb{Q})$. Let $\Gamma_{\mathbb{Q}}$ be the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$. Then we have a descent Kummer theory (see [**6**] and [**11**] for a general case).

Proposition 1.1 (Morton [**9**], Chapman [**1**], Ogawa [**11**], K [**6**]). *There exists a group isomorphism*

$$\delta : T(\mathbb{Q})/[3]T(\mathbb{Q}) \to \mathrm{Hom}_{\mathrm{cont}}(\Gamma_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z}).$$

In particular, for an $s \in \mathbb{Q}$ the field L_s is equal to $\overline{\mathbb{Q}}^{\mathrm{Ker}\delta(s)}$.

Corollary 1.2. *For rational numbers s_1 and $s_2 \in \mathbb{Q}$ the equation $L_{s_1} = L_{s_2}$ holds if and only if $\langle s_1 \rangle_T = \langle s_2 \rangle_T$ in $T(\mathbb{Q})/[3]T(\mathbb{Q})$.*

Corollary 1.3. *Assume that L_{s_1} and L_{s_2} are distinct cyclic cubic fields for rational numbers s_1 and $s_2 \in \mathbb{Q}$. Then two fields $L_{s_1 +_T s_2}$ and $L_{s_1 -_T s_2}$ are all of the cyclic cubic fields contained in the composite field $L_{s_1} L_{s_2}$ other than L_{s_1} and L_{s_2}.*

By using a result in [**6**] one can calculate the ramifications in $L_s/\mathbb{Q}$. We define U_3 by

$$U_3 = \{s \in \mathbb{Q} | v_3(s + 1/2) \leq -1 \text{ or } v_3(s + 1/2) \geq 2\}.$$

For a prime number $p \neq 3$, the set U_p is defined to be

$$U_p = \{s \in \mathbb{Q} | v_p(s^2 + s + 1) \leq 0 \text{ or } v_p(s^2 + s + 1) \equiv 0 \pmod 3\}.$$

Lemma 1.4 (K [**6**]). *For a rational number $s \in \mathbb{Q}$ the conductor f_{L_s} of the extension $L_s/\mathbb{Q}$ is equal to $\prod_p p^{\lambda_p}$ where*

$$\lambda_p = \begin{cases} 1 & \textit{if } p \neq 3 \textit{ and } s \notin U_p, \\ 2 & \textit{if } p = 3 \textit{ and } s \notin U_3, \\ 0 & \textit{otherwise.} \end{cases}$$

§ 2. Minimal element realizing a cyclic cubic field

Let us note that $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ is a principal ideal domain and $\mathcal{O}^{\times}_{\mathbb{Q}(\zeta)} = \langle -\zeta \rangle_{\mathbb{G}_m} \simeq \mathbb{Z}/6\mathbb{Z}$. Then it is easy to see

Lemma 2.1. *For a prime number p with $p \equiv 1 \pmod 3$ there exists a unique pair (a, b) of rational integers $a, b \in \mathbb{Z}$ such that $a^2 + ab + b^2 = p$, $b \equiv 0 \pmod 3$, $b > 0$ and $a/b \geq -1/2$.*

For a prime number $p \equiv 1 \pmod 3$ let a_p and b_p be the integers a and b satisfying all of the conditions in Lemma 2.1, respectively. For $p = 3$ we define $a_3 = 0$ and $b_3 = 1$. Now put $c_p = a_p/b_p \in \mathbb{Q}$.

Lemma 2.2. *The cyclic cubic field of prime conductor $p \equiv 1 \pmod 3$ is equal to L_{c_p}. The cyclic cubic field of conductor 9 is equal to L_{c_3}.*

Proof. For a prime number $p \equiv 1 \pmod 3$ we have $c_p^2 + c_p + 1 = p/b_p^2$. Then $v_p(c_p^2 + c_p + 1) = 1$ and $v_l(c_p^2 + c_p + 1) \leq 0$ for a prime number l with $l \neq p$. It follows from $v_3(b_p) \geq 1$ that $v_3(c_p + 1/2) = -v_3(b_p) \leq -1$. Thus Lemma 1.4 implies that L_{c_p} is a cyclic cubic field of conductor p. By class field theory there exists only one cyclic cubic field of conductor p. Thus the cyclic cubic field of conductor p is equal to L_{c_p}. In the same way we see that there exists only one cyclic cubic field of conductor 9, which is equal to L_{c_3}. □

Let N_3 be the set of all conductors of cyclic cubic fields. Then N_3 is equal to the set of positive integers $f \in \mathbb{Z}$, $f \geq 1$ such that

$$v_p(f) = \begin{cases} 0 \text{ or } 2 & \text{if } p = 3, \\ 0 \text{ or } 1 & \text{if } p \equiv 1 \pmod 3, \\ 0 & \text{otherwise,} \end{cases}$$

for every prime number p. Now fix an integer $f \in N_3$. Let $\mathcal{T}_f$ be the subset of $T(\mathbb{Q})$ consisting of elements of the form $\Sigma_T[m_p]c_p$ where p runs through all of the prime divisors of f and $m_p \in \{\pm 1\}$. Let $\mathcal{L}_f$ be the family of cyclic cubic fields with conductor f.

Proposition 2.3. *There exist a surjective map $R_{F,\mathbb{Q}} : \mathcal{T}_f \to \mathcal{L}_f$, $s \mapsto L_s$. In particular, $L_{s_1} = L_{s_2}$ for $s_1, s_2 \in \mathcal{T}_f$ if and only if $s_1 = s_2$ or $s_1 = -_T s_2$.*

By using Corollary 1.3 we see

Lemma 2.4. *Let $s_1, s_2 \in \mathbb{Q}$ with $s_1 +_T s_2 \neq \infty$. Assume that $L_{s_1}/\mathbb{Q}$ is unramified at a prime number p. Then p ramifies in $L_{s_1+_T s_2}/\mathbb{Q}$ if and only if so does in $L_{s_2}/\mathbb{Q}$.*

Proof of Proposition 2.3. Lemma 2.4 implies that for every $s \in \mathcal{T}_f$ the field L_s is cyclic cubic of conductor f. Thus the map $R_{F,\mathbb{Q}}$ is well-defined. Corollary 1.2 and Lemma 2.2 show that c_p are linearly independent in $T(\mathbb{Q})/[3]T(\mathbb{Q})$. Thus $\sharp\mathcal{T}_f = 2^r$ where r is the number of prime divisors of f. It follows from Corollary 1.2 and the linearly independency of c_p that $L_{s_1} = L_{s_2}$ for $s_1, s_2 \in \mathcal{T}_f$ if and only if $s_1 = s_2$ or $s_1 = -_T s_2$. By class field theory we have $\sharp\mathcal{L}_f = 2^{r-1}$. Hence the map $R_{F,\mathbb{Q}}$ is surjective. □

Let us define two subsets $\mathcal{T}_f^+$ and $\mathcal{T}_f^-$ of $\mathcal{T}_f$ such that $\mathcal{T}_f^+ = \{s \in \mathcal{T}_f | s \geq -1/2\}$ and $\mathcal{T}_f^- = \{s \in \mathcal{T}_f | s \leq -1/2\}$. Then $s \in \mathcal{T}_f^\pm$ holds if and only if so does $-_T s \in \mathcal{T}_f^\mp$, respectively. Indeed, $s + (-_T s) = -1$. Thus Proposition 2.3 verifies Theorem 0.1.

Let L be a cyclic cubic field of conductor $f = f_L$ and c_L a unique rational number $s \in \mathcal{T}_f^+$ such that $R_{F,\mathbb{Q}}(s) = L$. Let a_L and b_L be rational integers such that $a_L/b_L = c_L$, $\gcd(a_L, b_L) = 1$ and $b_L \geq 1$. Note that $a_L = a_p$, $b_L = b_p$ and $c_L = c_p$ if f is equal to a prime number p. We define $g_L = f_L/9$ if $3 \mid f_L$, and $g_L = f_L$ otherwise. One calls $g = g_L$ the tame conductor of L.

Lemma 2.5. *We have $g_L = a_L^2 + a_L b_L + b_L^2$.*

By the direct calculation one sees the following equation.

Lemma 2.6. *For $s_1 = \alpha_1/\beta_1$ and $s_2 = \alpha_2/\beta_2$ we have*

$$(s_1 +_T s_2)^2 + (s_1 +_T s_2) + 1 = \frac{(\alpha_1^2 + \alpha_1\beta_1 + \beta_1^2)(\alpha_2^2 + \alpha_2\beta_2 + \beta_2^2)}{(\alpha_1\beta_2 + \alpha_2\beta_1 + \beta_1\beta_2)^2}.$$

Proof of Lemma 2.5. It follows from the definition that $c_L^2 + c_L + 1 = (a_L^2 + a_L b_L + b_L^2)/b_L^2$. Note that $\gcd(a_L^2 + a_L b_L + b_L^2, b_L) = 1$. Lemma 2.6 implies that $(a_L^2 + a_L b_L + b_L^2) \mid g_L$. Indeed, $g_L = \prod_{p|f}(a_p^2 + a_p b_p + b_p^2)$. Let p be a prime divisor of g_L. Then $p \neq 3$ and $L/\mathbb{Q}$ is ramified at p. Lemma 1.4 means that $v_p(a_L^2 + a_L b_L + b_L^2) \geq 1$. Since g_L is square-free, one has $v_p(a_L^2 + a_L b_L + b_L^2) = v_p(g_L) = 1$. Thus we have $a_L^2 + a_L b_L + b_L^2 = g_L$. □

Let $H(s)$ be the Weil height of a rational number $s \in \mathbb{Q}$, that is, $H(s) = \max\{|\alpha|, |\beta|\}$ where $s = \alpha/\beta$ and $\alpha, \beta \in \mathbb{Z}$ with $\gcd(\alpha, \beta) = 1$. We note that $3H(s)^2/4 \leq \alpha^2 + \alpha\beta + \beta^2 \leq 3H(s)^2$. Let us define $H_L = \min\{H(s) | s \in T(\mathbb{Q}), L_s = L\}$. The genericity of $F(s, X)$ guarantees that $\{s \in T(\mathbb{Q}) | L_s = L\} \neq \emptyset$, and thus $H_L \in \mathbb{Z}$, $H_L \geq 1$. Let us denote $\{s \in T(\mathbb{Q}) | L_s = L, H(s) = H_L\}$ by $\mathcal{S}_L$.

Proposition 2.7. *If $c_L > 0$, then $\mathcal{S}_L = \{c_L\}$. If $c_L < 0$, then $\mathcal{S}_L = \{c_L, -_T c_L\}$. When $c_L = 0$, we have $L = L_{c_3}$ and $\mathcal{S}_L = \{0, 1, -1\}$.*

Corollary 2.8. *We have $H_L = H(c_L)$, that is, c_L has the minimal Weil height among rational numbers $s \in \mathbb{Q}$ such that $L_s = L$.*

Proof of Proposition 2.7. Let $s = \alpha/\beta \in \mathbb{Q}$ be an element in $\mathcal{S}_L$ where α and β are rational integers with $\gcd(\alpha, \beta) = 1$. Lemma 1.4 means that $g_L \mid (\alpha^2 + \alpha\beta + \beta^2)$. Let us denote by η_1 the ratio $(\alpha^2 + \alpha\beta + \beta^2)/g_L \in \mathbb{Z}$. It follows from the assumption

$H(s) \leq H(c_L)$ that $\eta_1 g_L \leq 3H(s)^2 \leq 4(3H(c_L)^2/4) \leq 4g_L$. Thus we have $\eta_1 \leq 4$. Since $\gcd(\alpha, \beta) = 1$, it holds that $v_2(\eta_1) = 0$. In fact, 2 remains prime in $\mathbb{Q}(\zeta)/\mathbb{Q}$. Thus $\eta_1 = 1$ or 3. Corollary 1.2 shows that $c_L {+_T} s \in [3]T(\mathbb{Q})$ or $c_L {-_T} s \in [3]T(\mathbb{Q})$. We first assume $t = c_L {+_T} s \in [3]T(\mathbb{Q})$ with $t \neq \infty$. Then Lemma 2.6 means that $t^2 + t + 1 = \eta_1 g_L^2/(a_L\beta + b_L\alpha + b_L\beta)^2$. Since $t \in [3]T(\mathbb{Q})$, we have $L_t = \mathbb{Q}$, that is, L_t is unramified at all primes. Thus one sees that $g_L \mid (a_L\beta + b_L\alpha + b_L\beta)$. Now put $\eta_2 = (a_L\beta + b_L\alpha + b_L\beta)/g_L \in \mathbb{Z}$. Then $t^2 + t + 1 = \eta_1/\eta_2^2$. It follows from $t \in \mathbb{Q}$ that $(t + 1/2)^2 = \eta_1/\eta_2^2 - 3/4 \geq 0$. Since $\eta_1 \in \{1, 3\}$ and $\eta_2 \in \mathbb{Z}$, we have $\eta_1/\eta_2^2 = 1$, 3 or 3/4. Then one sees that $t \in T_{\mathrm{tors}}(\mathbb{Q}) = \langle -2 \rangle_T \simeq \mathbb{Z}/6\mathbb{Z}$. Here, $T_{\mathrm{tors}}(\mathbb{Q}) \cap [3]T(\mathbb{Q}) = \{-1/2, \infty\}$. Thus we have $t = -1/2$ and $\eta_1/\eta_2^2 = 3/4$. This implies that $s = (-1/2) {-_T} c_L = (-a_L + b_L)/(2a_L + b_L)$. Then one sees that $H(s) = -a_L + b_L$ if $-1/2 \leq c_L \leq 0$, and $2a_L + b_L$ if $c_L \geq 0$. In fact, $\gcd(-a_L + b_L, 2a_L + b_L) = 1$ for $a_L \not\equiv b_L \pmod 3$. Then $H(s) \leq H(c_L)$ holds if and only if $a_L = 0$. When $a_L = 0$, we have $c_L = 0$ and $s = 1$. For the case $t = c_L {+_T} s = \infty$, one sees that $H(s) \leq H(c_L)$ implies $c_L \leq 0$. Conversely, if $c_L \leq 0$, then $H(-_T c_L) = H(c_L)$. In the same way as above we can show the assertion for the case $c_L {-_T} s \in [3]T(\mathbb{Q})$. □

Lemma 2.9. *We have* $1 < H_L/\sqrt{g_L/3} < 2$. *The lower (resp. the upper) bounds are the best possible, that is, for arbitrary positive real number* $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, *there exist infinitely many cyclic cubic fields* L *such that* $H_L/\sqrt{g_L/3} < 1 + \varepsilon$ *(resp.* $H_L/\sqrt{g_L/3} > 2 - \varepsilon$*).*

Proof. It follows from Lemma 2.5 and Corollary 2.7 that $3H_L^2/4 \leq g_L \leq 3H_L^2$, which shows the inequatilies in the first assertion. Let us consider a cyclic cubic field $L = L_{s_1}$ where $s_1 = (m+1)/m$ for a positive integer $m \in \mathbb{Z}$, $m \geq 1$. Then $s_1^2 + s_1 + 1 = \gamma(m)/m^2$ where $\gamma(Y) = 3Y^2 + 3Y + 1 \in \mathbb{Z}[Y]$. Now assume that $\gamma(m)$ is square-free. Then Lemma 1.4 implies that $g_L = \gamma(m)$. Since $3H_L^2 > g_L = \gamma(m)$, we have $H_L > m$. Thus $H_L = H(\alpha/\beta) = m + 1$ and $c_L = (m+1)/m \in \mathcal{T}_f^+$ where $f = \gamma(m)$ if $3 \mid m$ and $f = 9\gamma(m)$ otherwise. Then we have $3H_L^2/g_L = 3(m+1)^2/\gamma(m)$, which converges to 1 if m goes to $+\infty$. It follows from a result [**10**] of Nagell (cf. [**3**]) that there exist infinitely many positive integers $m \in \mathbb{Z}$ such that $\gamma(m)$ are square-free. Thus the lower bound is the best possible. Let us next consider a cyclic cubic field $L' = L_{s_2}$ where $s_2 = -m/(2m+1) = s_1 {+_T} 0$ and $\gamma(m)$ is square-free. Then one can see that $s_2 \in \mathcal{T}_{f'}^+$ where $f' = \gamma(m)$ if $m \equiv 1 \pmod 3$ and $f' = 9\gamma(m)$ otherwise. In fact, $c_3 = 0 \in T[3]$. Thus we have $H_{L'} = H(s_2) = 2m + 1$ and $3H_{L'}^2/g_{L'} = 3(2m+1)^2/\gamma(m)$, which converges to 4 if m goes to $+\infty$. Hence the upper bound is also the best possible. □

§ 3. Artin symbols of prime ideals for a cyclic polynomial

Let us assume that L_s is a cyclic cubic field for a rational number $s \in \mathbb{Q}$. Let x be a solution of $F(s, X) = 0$. Then $L_s = \mathbb{Q}(x)$ and $\mathrm{Gal}(L_s/\mathbb{Q}) = \langle \sigma \rangle$ where $\sigma(x) = x {+_T} (-1) = (-x - 1)/x$. Let p be a prime number with $p \neq 3$ and $v_p(s^2 + s + 1) \leq 0$. Lemma 1.4 implies that p is unramified in $L_s/\mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal of L_s above p. The Artin symbol (L_s/p) is defined to be an element $\tau \in \mathrm{Gal}(L_s/\mathbb{Q})$ such that $v_{\mathfrak{p}}(\alpha^p - \tau(\alpha)) \geq 1$ for every $\alpha \in \mathcal{O}_{L_s}$. Since $L_s/\mathbb{Q}$ is abelian, (L_s/p) depends not on the prime ideal $\mathfrak{p}$ but only on the prime number p.

We can define an algebraic torus $T(k)$ for a field k with positive characteristic $p \neq 3$ in the same way as the case of $\mathbb{Q}$ (cf. [**6**]). Note that $T(k) = k \cup \{\infty\} - \{\zeta, \zeta^{-1}\}$ where ζ is a primitive 3rd root of unity in $\overline{k}$.

Proposition 3.1. *If $p \equiv 1 \pmod 3$, then $(L_s/p) = \sigma^i$ where $i \in \mathbb{Z}$ is an integer satisfying $[i](-1) = [(p-1)/3]s$ in $T(\mathbb{F}_p)$. When $p \equiv 2 \pmod 3$, we have $(L_s/p) = \sigma^i$ for an integer $i \in \mathbb{Z}$ such that $[i](-1) = [(-p-1)/3]s$ in $T(\mathbb{F}_p)$.*

Lemma 3.2. *If $p \equiv \pm 1 \pmod 3$, then $[p]x = \pm_T x^p$ in $T(\mathbb{F}_\mathfrak{p})$, respectively.*

Proof. It follows from the definition that

$$[p]x = \frac{\zeta^{-1}(x-\zeta)^p - \zeta(x-\zeta^{-1})^p}{(x-\zeta)^p - (x-\zeta^{-1})^p}.$$

If $v_\mathfrak{p}(x) < 0$, then $v_\mathfrak{p}([p]x) < v_\mathfrak{p}(x) < 0$. Thus $[p]x = \pm_T x^p = \infty$ in $T(\mathbb{F}_\mathfrak{p})$. Now assume $v_\mathfrak{p}(x) \geq 0$. Then we have $[p]x \equiv \mathcal{B}_p(x) \pmod{\mathfrak{p}}$ where

$$\mathcal{B}_p(X) = \frac{(\zeta^{-1}-\zeta)X^p + (\zeta^{-p+1} - \zeta^{p-1})}{\zeta^{-p} - \zeta^p} \in \mathbb{Q}[X].$$

It is easy to see that $\mathcal{B}_p(X) = \pm_T X^p$ for $p \equiv \pm 1 \pmod 3$, respectively. □

Proof of Proposition 3.1. Let $i \in \mathbb{Z}$ be an integer such that $(L_s/p) = \sigma^i$. Then we have $x^p = \sigma^i(x)$ in $T(\mathbb{F}_\mathfrak{p})$ since $v_\mathfrak{p}(x^p - \sigma^i(x)) \geq 1$. Lemma 3.2 means that $\sigma^i(x) = [\pm p]x$ in $T(\mathbb{F}_\mathfrak{p})$ for $p \equiv \pm 1 \pmod 3$, respectively. Note that $\sigma^i(x) = x +_T [i](-1)$ and $[3]x = s$. Thus we have $[i](-1) = [\pm p]x -_T x = [\pm p - 1]x = [(\pm p - 1)/3]s$ in $T(\mathbb{F}_\mathfrak{p})$. Here $i, (\pm p - 1)/3 \in \mathbb{Z}$ and $-1, s \in T(\mathbb{F}_p)$. Thus we have an equation $[i](-1) = [(\pm p - 1)/3]s$ in $T(\mathbb{F}_p)$, which uniquely determines σ^i in $\mathrm{Gal}(L_s/\mathbb{Q})$. In fact, the order of -1 in $T(\mathbb{F}_p)$ and that of σ in $\mathrm{Gal}(L_s/\mathbb{Q})$ are both equal to 3. □

Proposition 3.3. *For an $s \in \mathbb{Q}$ the decomposition of* 3 *in the extension $L_s/\mathbb{Q}$ is as follows*:
(i) 3 *ramifies in $L_s/\mathbb{Q}$ if and only if* $0 \leq v_3(s + 1/2) \leq 1$.
(ii) 3 *splits completely in $L_s/\mathbb{Q}$ if and only if* $v_3(s) \leq -2$ *or* $v_3(s+1/2) \geq 3$.
(iii) 3 *remains prime in $L_s/\mathbb{Q}$ if and only if* $v_3(s) = -1$ *or* $v_3(s+1/2) = 2$. *When* $v_3(s) = -1$ *and* $3s \equiv \mp 1 \pmod 3$, *we have* $(L_s/3) = \sigma^{\pm 1}$, *respectively. For the case* $v_3(s+1/2) = 2$ *and* $(s+1/2)/9 \equiv \pm 1 \pmod 3$, *it satisfies* $(L_s/3) = \sigma^{\pm 1}$, *respectively.*

Proof. Lemma 1.4 implies the assertion (i). If $v_3(s) = -(\nu+1) \leq -2$ for a positive integer $\nu \in \mathbb{Z}$ with $\nu \geq 1$, then $F_\nu(u,Y) = F(u/3^{\nu+1}, Y/3^\nu)3^{3\nu} \equiv Y^3 - uY^2 \pmod 3$ where $u = 3^{\nu+1}s \in \mathbb{Q}$ and $v_3(u) = 0$. Note that $F_\nu(u,u) \equiv 0 \pmod 3$ and $\partial F_\nu(u,Y)/\partial Y|_{Y=u} \equiv u^2 \not\equiv 0 \pmod 3$. Hensel's lemma implies that there exists a solution $Y = \tilde{u} \in \mathbb{Z}_p$ of $F_\nu(u,Y) = 0$. Then $x_1 = 3^\nu \tilde{u} \in \mathbb{Q}_p$ is a solution of $F(s,X) = 0$. Let us put $x_2 = x_1 +_T (-1)$ and $x_3 = x_1 +_T 0$. Then $x_2, x_3 \in \mathbb{Q}_p$ are solutions of $F(s,X) = 0$ such that $v_3(x_2) = -\nu$ and $v_3(x_3) = 0$. This means that $F(s,X) = (X-x_1)(X-x_2)(X-x_3)$ in $\mathbb{Q}_p$, that is, p splits completely in $L_s/\mathbb{Q}$. Now assume $v_3(s) = -1$. Then $F(s,X)$ is defined over $\mathbb{Z}_3$, and $F(s,X) \equiv X^3 \mp (X^2+X) - 1 \pmod 3$ if $3s \equiv \pm 1 \pmod 3$, respectively. Here $X^3 \mp (X^2+X) - 1$ are irreducible over $\mathbb{F}_3$. Thus 3 remains prime in $L_s/\mathbb{Q}$. By the direct calculation one sees that $X^3 - (-X-1)/X \equiv (X-1)(X^3+X^2+X-1)/X$

(mod 3). For a solution $x \in \overline{\mathbb{Q}_p}$ of $F(s, X) = 0$ with $3s \equiv -1 \pmod 3$, we have $v_{\mathfrak{p}}(x^3 - \sigma(x)) \geq 1$ where $\mathfrak{p} = (3)$ is the prime ideal of L_s above 3. Indeed, $v_{\mathfrak{p}}(x) = 0$. In the same way as above, one has $(L_s/3) = \sigma^2$ when $3s \equiv 1 \pmod 3$. Now put $s_1 = s +_T (-1/2) = (-s-2)/(2s+1)$. It follows from Proposition 1.1 that $L_s = L_{s_1}$ since $-1/2$ is a 2-torsion element. If $v_3(s + 1/2) \geq 3$, then $v_3(s_1) \leq -2$. Thus 3 splits completely in $L_s = L_{s_1}$. When $v_3(s + 1/2) = 2$, we have $v_3(s_1) = -1$. Now set $\epsilon = (s+1/2)/9 \in \mathbb{Z}_3^\times$. Then $3s_1 + \epsilon = (4\epsilon^2 - 6\epsilon - 1)/(4\epsilon) \equiv 0 \pmod 3$. By using the assertion of the case $v_3(s) = -1$ one can have that $\epsilon \equiv \pm 1 \pmod 3$ implies $(L_s/3) = \sigma^{\pm 1}$, respectively. □

§ 4. Ring of integers of a cyclic cubic field

Let L be a cyclic cubic field of conductor f_L, and $\mathcal{O}_L$ the ring of integers of L. Let x be a solution of $F(c_L, X) = 0$.

Lemma 4.1. *If $3 \nmid f_L$, then $\mathcal{O}_L$ is generated by 1, $b_L x/3$ and $b_L \sigma(x)/3$ as $\mathbb{Z}$-module. When $3 \mid f_L$, we have $\mathcal{O}_L = \mathbb{Z} + \mathbb{Z} b_L x + \mathbb{Z} b_L \sigma(x)$.*

Proof. Let us assume $3 \nmid f_L$. We first show that $b_L x/3$ and $b_L \sigma(x)/3$ are algebraic integers in L. The minimal polynomial of $y = b_L x/3$ over $\mathbb{Q}$ is equal to $Y^3 - a_L Y^2 - (a_L + b_L)(b_L/3)Y - (b_L/3)^3$. It follows from the construction of $\mathcal{T}_f$ that $v_3(b_L) \geq 1$ and $b_L/3 \in \mathbb{Z}$. Thus $y \in \mathcal{O}_L$ holds and so does $\sigma(y) = b_L \sigma(x)/3 \in \mathcal{O}_L$. Let R be a submodule of $\mathcal{O}_L$ generated by $\{1, b_L x/3, b_L \sigma(x)/3\}$ as $\mathbb{Z}$-module. Since $b_L \sigma(x)/3 = -b_L x^2/3 + a_L x + a_L + 2b_L/3$, the module R is generated by $\{1, b_L x/3, b_L x^2/3 - a_L x\}$ as $\mathbb{Z}$-module. Here the discriminant of the element x is equal to $3^4(c_L^2 + c_L + 1)^2 = g_L^2 (b_L/3)^{-4}$. Thus the discriminant of R is equal to g_L^2. It follows from $3 \nmid f_L$ that the discriminant of $\mathcal{O}_L$ is equal to g_L^2. This shows that $R = \mathcal{O}_L$. In the same way as above one can see that $\mathcal{O}_L = \mathbb{Z} + \mathbb{Z} b_L x + \mathbb{Z}(b_L x^2 - 3a_L x)$ for the case $3 \mid f_L$. □

Corollary 4.2. *If $3 \nmid f_L$ and $b_L = 3$, then $\mathcal{O}_L = \mathbb{Z}[x]$, that is, $\mathcal{O}_L$ has a power basis. When $3 \mid f_L$ and $b_L = 1$, we have $\mathcal{O}_L = \mathbb{Z}[x]$.*

By the direct calculation we have

$$F(c_L, (X + a_L)/b_L) b_L^3 = X^3 - 3g_L X - (2a_L + b_L) g_L,$$

which is the same polynomial described in [**2**]. In §6.4.2 of [**2**] one can see the same statement as that of Lemma 4.1

§ 5. Numerical examples for cyclic cubic fields

For prime numbers $p = 3$ and $p \equiv 1 \pmod 3$ with $p \leq 1000$ we calculate the numbers $c_p = a_p/b_p$ where a_p and b_p satisfy all of the conditions in Lemma 2.1. The data is contained in Table 5.1 below. For an integer $f = 482391 = 3^2 \times 7 \times 13 \times 19 \times 31$ we compute the set $\mathcal{T}_f$. There exist $2^{5-1} = 16$ cyclic cubic fields of conductor f. For all such fields L we denote the numbers c_L in the c_L-column of Table 5.2. At the coordinates (c_L, p) of the left part in Table 5.2 we denote the signs ± of the numbers $m_p \in \{\pm 1\}$ such that $c_L = \Sigma_{T\,p|f}[m_p]c_p$, respectively. The number at (c_L, p) of the right part in Table 5.2 is equal to

$$\begin{cases} \quad 0 & \text{if } p \text{ splits completely in } L/\mathbb{Q}, \\ 1 \text{ and } 2 & \text{if } p \text{ remains prime in } L/\mathbb{Q} \text{ with } (L_s/p) = \sigma \text{ and } \sigma^2, \text{ respectively}, \\ \quad 3 & \text{if } p \text{ ramifies in } L/\mathbb{Q}. \end{cases}$$

For example, there exists a number 1 at $(c_L, p) = (3/230, 17)$. This means that 17 remains prime in $L = L_{3/230}$ and $(L/17) = \sigma$ where $\sigma(x) = (-x-1)/x$ for $x \in L$ with $F(3/230, x) = 0$. From the data of the numbers m_p we have already known that all of the 16 fields in Table 5.2 are distinct from each other. The data of the Artin symbols is useful to find $s \in \mathbb{Q}$ corresponding to a field L whose definition polynomial is not of the type $F(t, X)$. The data at the right part of Table 5.2 itself enables us to distinguish the 16 fields completely. Let M be the minimal splitting field of $A(Z) = Z^3 - 160797Z - 24709139$ over $\mathbb{Q}$. Since the discriminant of the polynomial $A(Z)$ is equal to a square $145438173050625 = 3^4 5^4 7^2 13^2 19^2 31^2$, the field M is cyclic cubic over $\mathbb{Q}$ or is equal to $\mathbb{Q}$. It follows from some method (cf. [**8**]) that the set of prime numbers ramifying in $M/\mathbb{Q}$ are $\{3, 7, 13, 19, 31\}$. Thus M is a cyclic cubic field of conductor $f = 482391$. One can calculate a generator $\tau \in \mathrm{Gal}(M/\mathbb{Q})$ such that $\tau(z) = (-218z - 53599)/(z + 243)$ for $z \in M$ with $A(z) = 0$. One can check that

$$(M/2) = \tau^2, (M/5) = \mathrm{id}, (M/11) = \tau, (M/17) = \tau^2, (M/23) = \tau, (M/29) = \tau^2.$$

By comparing the data in Table 5.2 and above at the primes $p = 2, 5, 11$ and 17, we have $M = L_{218/25}$. Note that the Artin symbols are determined uniquely up to the choice of the generator of $\mathrm{Gal}(M/\mathbb{Q})$. In fact, $A(Z)$ is equal to $F(c_L, (Z + a_L)/b_L) b_L^3$ for $c_L = 218/25$.

p	c_p	p	c_p	p	c_p	p	c_p
3	0	199	$-2/15$	439	$5/18$	727	$13/18$
7	$-1/3$	211	$-1/15$	457	$-7/24$	733	$19/12$
13	$1/3$	223	$11/6$	463	$1/21$	739	$-7/30$
19	$2/3$	229	$5/12$	487	$2/21$	751	$10/21$
31	$-1/6$	241	$1/15$	499	$7/18$	757	$1/27$
37	$4/3$	271	$10/9$	523	$17/9$	769	$17/15$
43	$1/6$	277	$7/12$	541	$4/21$	787	$2/27$
61	$-4/9$	283	$13/6$	547	$-13/27$	811	$25/6$
67	$-2/9$	307	$-1/18$	571	$5/21$	823	$-14/33$
73	$-1/9$	313	$16/3$	577	$-8/27$	829	$-13/33$
79	$7/3$	331	$-10/21$	601	$1/24$	853	$4/27$
97	$8/3$	337	$-8/21$	607	$23/3$	859	$-10/33$
103	$2/9$	349	$17/3$	613	$19/9$	877	$28/3$
109	$-5/12$	367	$13/9$	619	$-5/27$	883	$13/21$
127	$7/6$	373	$-4/21$	631	$14/15$	907	$-7/33$
139	$10/3$	379	$7/15$	643	$11/18$	919	$17/18$
151	$5/9$	397	$11/12$	661	$20/9$	937	$29/3$
157	$1/12$	409	$8/15$	673	$8/21$	967	$7/27$
163	$11/3$	421	$-1/21$	691	$-11/30$	991	$26/9$
181	$-4/15$	433	$-11/24$	709	$25/3$	997	$-13/36$
193	$7/9$						

Table 5.1 (c_p for $p \leq 1000$)

3	7	13	19	31	c_L	2	3	5	7	11	13	17	19	23	29
+	−	+	−	+	$3/230$	0	3	0	3	0	3	1	3	0	1
−	−	−	−	−	$-43/250$	0	3	0	3	1	3	1	3	1	1
−	−	+	+	+	$197/58$	0	3	1	3	1	3	0	3	0	0
−	−	−	−	+	$145/122$	0	3	2	3	0	3	2	3	1	1
−	+	−	+	+	$-85/262$	0	3	2	3	2	3	0	3	0	2
−	−	+	+	−	$25/218$	0	3	2	3	2	3	2	3	0	0
+	−	−	+	−	$-102/265$	1	3	0	3	0	3	0	3	0	1
−	+	+	+	−	$122/145$	1	3	0	3	1	3	1	3	1	0
−	+	−	−	+	$218/25$	1	3	0	3	2	3	1	3	2	1
−	+	−	−	−	$58/197$	1	3	1	3	0	3	0	3	2	1
+	+	+	−	+	$102/163$	1	3	1	3	2	3	0	3	1	1
+	+	+	−	−	$-90/263$	1	3	2	3	0	3	2	3	1	1
+	−	−	+	+	$90/173$	1	3	2	3	2	3	1	3	0	1
+	+	−	+	+	$177/85$	2	3	0	3	1	3	0	3	1	1
+	−	−	−	−	$207/43$	2	3	1	3	0	3	1	3	2	0
+	+	−	+	−	$-3/233$	2	3	1	3	2	3	2	3	1	1

Table 5.2 (16 cyclic cubic fields of conductor 482391)

References

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

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

[3] T.W. Cusick, *Lower bounds for regulators*, Lecture Notes in Math. **1068** (1984), 63–73.

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

[5] M. Kida, *Kummer theory for norm algebraic tori*, in preparation. (talk at Algebraic Number Theory and Related Topics (RIMS) on December 6-10, 2004.)

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

[7] T. Komatsu, *On arithmetic properties of a generic dihedral polynomial*, in preparation.

[8] P. Llorente, E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87** (1983), no. 4, 579–585.

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

[10] T. Nagell, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 178–193.

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

[12] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. **130** (2002), no. 8, 2215–2218.

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

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

[15] N. Suwa, *Twisted Kummer and Kummer-Artin-Schreier theories*, in preparation. (talk at Algebraic Number Theory and Related Topics (RIMS) on December 6-10, 2004.)

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

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

List of MHF Preprint Series, Kyushu University

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MHF2004-11 Raimundas VIDŪNAS
Transformations of Gauss hypergeometric functions

MHF2004-12 Koji NAKAGAWA & Masakazu SUZUKI
Mathematical knowledge browser

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

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

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

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

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

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

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

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

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

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

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

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

MHF2004-25 Raimundas VIDŪNAS
Degenerate Gauss hypergeometric functions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MHF2005-12 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