TOKYO J. MATH.
VOL. 30, NO. 1, 2007

Cyclic Cubic Field with Explicit Artin Symbols

Toru KOMATSU

Kyushu University

(Communicated by K. Ota)

Abstract. In this paper we present a set $\mathcal{T}_f^+$ of rational numbers $s \in \mathbf{Q}$ 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 $s \in \mathbf{Q}$ such that $L_s = L$. If a cyclic cubic field L of conductor f is given, then we can choose the number $s \in \mathcal{T}_f^+$ 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] have generalized the polynomial $F(t, X)$ to the cases of general degree, and the author [6] studied the arithmetic properties of the general degree cases. For a rational number $s \in \mathbf{Q}$ let L_s be the minimal splitting field of $F(s, X)$ over $\mathbf{Q}$. We give a method for making a rational number $s \in \mathbf{Q}$ 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 $a_p/b_p \in \mathbf{Q}$ by c_p where (a_p, b_p) is a unique pair in the set $\{(a, b) \in \mathbf{Z} \times \mathbf{Z} | a^2 + ab + b^2 = p,\ b \equiv 0 \pmod 3,\ b > 0 \text{ and } a/b \geq -1/2\}$. Put $c_3 = 0$. In a previous paper [6] we defined an algebraic torus $T(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$ 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 $T(\mathbf{Q})$ consisting of elements of the form $\Sigma_T [m_p] c_p$ where p runs through all of the prime divisors of f and $m_p \in \{\pm 1\}$ (see [6] or § 1 for the definition of $[\pm 1]$). 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.

Received July 29, 2005; revised December 26, 2005

THEOREM 0.1 (Proposition 2.3 in § 2). *There exists a one-to-one correspondence* $R_{F,\mathbf{Q}} : \mathcal{T}_f^+ \to \mathcal{L}_f,\ s \mapsto L_s$.

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

PROPOSITION 0.2 (Corollary 2.8 in § 2). *The Weil's height of the number* c_L *is minimal among all of the rational numbers* $s \in \mathbf{Q}$ *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 $s \in \mathbf{Q}$ in $\mathcal{T}_f^+$ for the given cyclic cubic field L. To determine the number s in $\mathcal{T}_f^+$ corresponding to L we calculate the Artin symbols. Now assume that $L_s/\mathbf{Q}$ is cubic for a rational number $s \in \mathbf{Q}$. Let σ be a generator of $\mathrm{Gal}(L_s/\mathbf{Q})$ 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 $L_s/\mathbf{Q}$. We define $\mu_p(s) = v_p(s^2+s+1)$ where v_p is the normalized p-adic additive valuation. One 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 $\mathbf{Q}$ (cf. §3 or [6]).

THEOREM 0.4 (Proposition 3.1 in § 3). *Assume that* $p \neq 3$. *If* $\mu_p(s) < 0$, *then* $(L_s/p) = \mathrm{id}$, *that is*, p *splits completely in* $L_s/\mathbf{Q}$. *For the case* $\mu_p(s) = 0$, *we have* $(L_s/p) = \sigma^i$ *where* $i \in \mathbf{Z}$ *is an integer such that* $[i](-1) = [(\pm p - 1)/3]s$ *in* $T(\mathbf{F}_p)$ *provided* $p \equiv \pm 1 \pmod 3$, *respectively*. *When* $\mu_p(s) > 0$ *and* $\mu_p(s) \not\equiv 0 \pmod 3$, $L_s/\mathbf{Q}$ *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 show Theorem 0.4 for the general degree cases in the same way as the proof of Proposition 3.1.

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 give a remark on generators for the ring of integers of the cyclic cubic field L_s as $\mathbf{Z}$-module. In §5 we exhibit some numerical examples.

Acknowledgement. The author expresses his thanks to the editor Professor Kaori Ota for many valuable advice on the manuscript. He is grateful to the referee for many helpful comments and careful reading of the manuscript. He is supported by the 21st Century COE Program "Development of Dynamic Mathematics with High Functionality".

1. Preparation

We recall some results in the paper [6]. Let $T(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$ 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 $\varphi : T \to \mathbf{G}_m$, $t \mapsto (t-\zeta)/(t-\zeta^{-1})$ over $\mathbf{Q}(\zeta)$ 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 $m \in \mathbf{Z}$ 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 $[m]T(\mathbf{Q}) = \{[m]s | s \in T(\mathbf{Q})\}$ and $T[m] = T(\bar{\mathbf{Q}})[m] = \{x \in T(\bar{\mathbf{Q}}) | [m]x = \infty\}$. Note that $T[3] = \langle -1 \rangle_T = \{\infty, -1, 0\} \subset T(\mathbf{Q})$. Let $\Gamma_{\mathbf{Q}}$ be the absolute Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ of $\mathbf{Q}$. Then we have a descent Kummer theory (see [6] and [11] for general cases).

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

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

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

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

COROLLARY 1.3. *Assume that L_{s_1} and L_{s_2} are distinct cyclic cubic fields for rational numbers s_1 and $s_2 \in \mathbf{Q}$. 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 $L_s/\mathbf{Q}$. For a prime number $p \neq 3$, we define U_p by

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

The set U_3 is defined to be

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

LEMMA 1.4 (Komatsu [6]). *For $s \in \mathbf{Q}$ the conductor f_{L_s} of the extension $L_s/\mathbf{Q}$ 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 the ring of integers $\mathcal{O}_{\mathbf{Q}(\zeta)} = \mathbf{Z}[\zeta]$ is a principal ideal domain and $\mathcal{O}^{\times}_{\mathbf{Q}(\zeta)} = \langle -\zeta \rangle_{\mathbf{G}_m} \simeq \mathbf{Z}/6\mathbf{Z}$. 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 $a, b \in \mathbf{Z}$ 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 $c_p = a_p/b_p \in \mathbf{Q}$.

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 $f \in \mathbf{Z}$, $f \geq 1$ such that

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

for every prime number p. Now fix an integer $f \in N_3$. Let $\mathcal{T}_f$ be the subset of $T(\mathbf{Q})$ 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 exists a surjective map* $R_{F,\mathbf{Q}} : \mathcal{T}_f \to \mathcal{L}_f,\ s \mapsto L_s$. *Moreover*, $L_{s_1} = L_{s_2}$ *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* $s_1, s_2 \in \mathbf{Q}$ *with* $s_1 +_T s_2 \neq \infty$. *Assume that* $L_{s_1}/\mathbf{Q}$ *is unramified at a prime number* p. *Then* p *ramifies in* $L_{s_1+_T s_2}/\mathbf{Q}$ *if and only if so does in* $L_{s_2}/\mathbf{Q}$.

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 $R_{F,\mathbf{Q}}$ is well-defined. Corollary 1.2 and Lemma 2.2 show that c_p are linearly independent in $T(\mathbf{Q})/[3]T(\mathbf{Q})$. Thus $\sharp\mathcal{T}_f = 2^r$ where $\sharp S$ denotes the number of elements in a set S and r is the number of prime divisors of f. From Corollary 1.2 and the linear independence of c_p, it follows 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 $R_{F,\mathbf{Q}}$ 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 be a unique rational number $s \in \mathcal{T}_f^+$ such that $R_{F,\mathbf{Q}}(s) = L$. 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, $g_L = \prod_{p \mid f}(a_p^2 + a_p b_p + b_p^2)$. Let p be a prime divisor of g_L. Then $p \neq 3$ and $L/\mathbf{Q}$ 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 $s \in \mathbf{Q}$, that is, $H(s) = \max\{|\alpha|, |\beta|\}$ where $s = \alpha/\beta$ and $\alpha, \beta \in \mathbf{Z}$ 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 $H_L = \min\{H(s) | s \in T(\mathbf{Q}), L_s = L\}$. The genericity of $F(s, X)$ guarantees that $\{s \in T(\mathbf{Q}) | L_s = L\} \neq \emptyset$, and thus $H_L \in \mathbf{Z}$, $H_L \geq 1$. Let us denote $\{s \in T(\mathbf{Q}) | L_s = L, H(s) = H_L\}$ 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* $s \in \mathbf{Q}$ *such that* $L_s = L$.

PROOF OF PROPOSITION 2.7. Let $s = \alpha/\beta \in \mathbf{Q}$ 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 $(\alpha^2 + \alpha\beta + \beta^2)/g_L \in \mathbf{Z}$. 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 $\mathbf{Q}(\zeta)/\mathbf{Q}$. Thus $\eta_1 = 1$ or 3. Corollary 1.2 shows that $c_L +_T s \in [3]T(\mathbf{Q})$ or $c_L -_T s \in [3]T(\mathbf{Q})$. We first assume $t = c_L +_T s \in [3]T(\mathbf{Q})$ 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 $t \in [3]T(\mathbf{Q})$, we have $L_t = \mathbf{Q}$, 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 $\eta_2 = (a_L\beta + b_L\alpha + b_L\beta)/g_L \in \mathbf{Z}$. Then $t^2 + t + 1 = \eta_1/\eta_2^2$. It follows from $t \in \mathbf{Q}$ that $(t + 1/2)^2 = \eta_1/\eta_2^2 - 3/4 \geq 0$. Since $\eta_1 \in \{1, 3\}$ and $\eta_2 \in \mathbf{Z}$, we have $\eta_1/\eta_2^2 = 1$, 3 or $3/4$. Then one sees that $t \in T_{\mathrm{tors}}(\mathbf{Q}) = \langle -2 \rangle_T \simeq \mathbf{Z}/6\mathbf{Z}$. Here,

$T_{\text{tors}}(\mathbf{Q}) \cap [3]T(\mathbf{Q}) = \{-1/2, \infty\}$. 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 $-1/2 \le c_L \le 0$, and $2a_L + b_L$ if $c_L \ge 0$. In fact, $\gcd(-a_L + b_L, 2a_L + b_L) = 1$ for $a_L \not\equiv b_L \pmod 3$. Then $H(s) \le H(c_L)$ 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 $H(s) \le H(c_L)$ implies $c_L \le 0$. Conversely, if $c_L \le 0$, then $H(-_T c_L) = H(c_L)$. In the same way as above we can show the assertion for the case $c_L -_T s \in [3]T(\mathbf{Q})$. □

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* $\varepsilon \in \mathbf{R}$, $\varepsilon > 0$, *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 $3H_L^2/4 \le g_L \le 3H_L^2$, which shows the inequalities 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 $m \in \mathbf{Z}$, $m \ge 1$. Then $s_1^2 + s_1 + 1 = \gamma(m)/m^2$ where $\gamma(Y) = 3Y^2 + 3Y + 1 \in \mathbf{Z}[Y]$. 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 $m \in \mathbf{Z}$ 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 $s \in \mathbf{Q}$. Let x be a solution of $F(s, X) = 0$. Then $L_s = \mathbf{Q}(x)$ and $\mathrm{Gal}(L_s/\mathbf{Q}) = \langle\sigma\rangle$ where $\sigma(x) = x +_T (-1) = (-x-1)/x$. Let p be a prime number with $p \ne 3$ and $v_p(s^2 + s + 1) \le 0$. Lemma 1.4 implies that p is unramified in $L_s/\mathbf{Q}$. Let $\mathfrak{p}$ be a prime ideal of L_s above p. The Artin symbol (L_s/p) is defined to be an element $\tau \in \mathrm{Gal}(L_s/\mathbf{Q})$ such that $v_{\mathfrak{p}}(\alpha^p - \tau(\alpha)) \ge 1$ for every $\alpha \in \mathcal{O}_{L_s}$. Since $L_s/\mathbf{Q}$ is abelian, (L_s/p) depends not on the choice of 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 $p \ne 3$ in the same way as the case of $\mathbf{Q}$ (cf. [6]). Note that $T(k) = k \cup \{\infty\} - \{\zeta, \zeta^{-1}\}$ where ζ is a primitive 3rd root of unity in $\bar{k}$.

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

LEMMA 3.2. *If* $p \equiv \pm 1 \pmod 3$, *then* $[p]x = \pm_T x^p$ *in* $T(\mathbf{F}_{\mathfrak{p}})$, *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 $T(\mathbf{F}_{\mathfrak{p}})$. Now assume $v_{\mathfrak{p}}(x) \geq 0$. Then we have $[p]x \equiv \mathcal{B}_p(x) \pmod{\mathfrak{p}}$ where

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

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

PROPOSITION 3.3. *For any* $s \in \mathbf{Q}$ *the decomposition of* 3 *in the extension* $L_s/\mathbf{Q}$ *is as follows*:

(i) 3 *ramifies in* $L_s/\mathbf{Q}$ *if and only if* $0 \leq v_3(s + 1/2) \leq 1$.

(ii) 3 *splits completely in* $L_s/\mathbf{Q}$ *if and only if* $v_3(s) \leq -2$ *or* $v_3(s + 1/2) \geq 3$.

(iii) 3 *remains prime in* $L_s/\mathbf{Q}$ *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 $\nu \in \mathbf{Z}$ 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 $u = 3^{\nu+1}s \in \mathbf{Q}$ 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 $Y = \tilde{u} \in \mathbf{Z}_p$ of $F_\nu(u, Y) = 0$. Then $x_1 = 3^\nu \tilde{u} \in \mathbf{Q}_p$ 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 $x_2, x_3 \in \mathbf{Q}_p$ 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 $\mathbf{Q}_p$, that is, p splits completely in $L_s/\mathbf{Q}$. Now assume $v_3(s) = -1$. Then $F(s, X)$ is defined over $\mathbf{Z}_3$, 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 $\mathbf{F}_3$. Thus 3 remains prime in $L_s/\mathbf{Q}$. By the direct calculation one sees that $X^3 - (-X - 1)/X \equiv (X - 1)(X^3 + X^2 + X - 1)/X \pmod 3$. For a solution $x \in \bar{\mathbf{Q}}_p$ 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 in $T(\mathbf{Q})$. 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 $\varepsilon = (s+1/2)/9 \in \mathbf{Z}_3^\times$. Then $3s_1 + \varepsilon = (4\varepsilon^2 - 6\varepsilon - 1)/(4\varepsilon) \equiv 0 \pmod 3$. By using the assertion of the case $v_3(s) = -1$ one can have that $\varepsilon \equiv \pm 1 \pmod 3$ 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* $\mathbf{Z}$*-module*. *When* $3 \mid f_L$, *we have* $\mathcal{O}_L = \mathbf{Z} + \mathbf{Z}b_L x + \mathbf{Z}b_L\sigma(x)$.

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 $\mathbf{Q}$ 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 $b_L/3 \in \mathbf{Z}$. 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 $\mathbf{Z}$-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 $\mathbf{Z}$-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 $\mathcal{O}_L = \mathbf{Z} + \mathbf{Z}b_L x + \mathbf{Z}(b_L x^2 - 3a_L x)$ for the case $3 \mid f_L$. □

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

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 $\pm$ of the numbers $m_p \in \{\pm 1\}$ such that $c_L = \sum_{T\, p|f} [m_p] c_p$, respectively. The numbers 0, 1, 2, 3 at (c_L, p) of the right part in Table 5.2 represent

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

TABLE 5.1 (c_p for $p \le 1000$)

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 5.2 (16 cyclic cubic fields of conductor 482391)

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

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 $s \in \mathbf{Q}$ 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 $\mathbf{Q}$. 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 $\mathbf{Q}$ or is equal to $\mathbf{Q}$. It follows from some method (cf. [8]) that the set of prime numbers ramifying in $M/\mathbf{Q}$ are $\{3, 7, 13, 19, 31\}$. Thus M is a cyclic cubic field of conductor $f = 482391$. One can calculate a generator $\tau \in \mathrm{Gal}(M/\mathbf{Q})$ 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 $\mathrm{Gal}(M/\mathbf{Q})$. In fact, $A(Z)$ is equal to $F(c_L, (Z + a_L)/b_L)b_L^3$ for $c_L = 218/25$.

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, J. Algebra **293** (2005), no. 2, 427–447.

[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 (Japanese), Algebraic number theory and related topics (Kyoto, 2004). Surikaisekikenkyusho Kokyuroku **1451** (2005), 243–256.

Present Address:
Department of Mathematics, Sophia University,
Kioi-cyo, Chiyoda-ku, Tokyo, 102–8554 Japan.
e-mail: trkomatu@mm.sophia.ac.jp