Doctoral Thesis
Doctor of Science

Relative power integral bases for cyclic extensions

（巡回拡大の相対冪整基底について）

Ryutaro Sekigawa
（関川　隆太郎）

March, 2022

Department of Mathematics
Graduate School of Science and Technology
Tokyo University of Science

Contents

Chapter 1

Introduction

An *algebraic number field* is a finite field extension K of the rational number field $\mathbb{Q}$. The elements of K are called *algebraic numbers.* An algebraic number is an *algebraic integer* if it is a root of a monic polynomial with integer coefficients. The *ring of integers* $\mathcal{O}_K$ of K is the ring of all algebraic integers of K. Any rational number is an algebraic number and the ring of integers of $\mathbb{Q}$ is equal to the rational integer ring $\mathbb{Z}$. Let n be the degree of K. Then it is said that an element α of K generates a *power integral basis* if it holds that

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} \mid x_i \in \mathbb{Z}\}.$$

In such a case, we say that K is *monogenic.*

The main results in this paper are

- We give concise and explicit equivalent conditions for the monogenity of cyclic cubic fields (Theorem 2.5.1 in Chapter 2).
- We give a sufficient condition for the monogenity of relative cyclic extensions of prime degree and provide families of infinitely many monogenic cyclic extensions (Theorems 3.2.1, 3.5.1 in Chapter 3).

In algebraic number theory, the study of algebraic number fields and various invariants associated with algebraic number fields has been performed. In particular, it is a classical problem to determine whether K has a power integral basis. In the 1960s, Hasse proposed to characterize algebraic number fields that have power integral bases, which is now called Hasse's problem. On the other hand, the problem is equivalent to investigating integer solutions to an equation for the discriminant of K. In other words, Hasse's problem can be regarded as solving Diophantine equations. For simplicity, we assume that $K/\mathbb{Q}$ is a Galois extension. Then $\alpha \in K$ provides a power integral basis if and only if it holds that

$$\pm d_K = d_K(\alpha) := N_{K/\mathbb{Q}}\left(\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})\setminus\{id\}} (\alpha - \sigma(\alpha))\right)$$

where d_K is the discriminant of K. Historically, the study on power integral bases is actually related to the study on solving Diophantine equations. For example, a method to determine power integral bases of cubic fields has been obtained as an application of a method of solving for Thue equation. On the other hand, there are many direct applications of power integral bases. A simple example is that, by obtaining the generator α of a power integral basis of K of degree n, an arbitrary element of $\mathcal{O}_K$ can be uniquely expressed as a polynomial of α with integer coefficients of degree less than n. Furthermore, this expression allows explicit calculation in $\mathcal{O}_K$, especially multiplication.

We present some examples and previous research. Quadratic fields, cyclotomic fields, and the maximal real subfields of cyclotomic fields are classically important in number theory, and all of these fields have power integral bases. The first non-monogenic example was given by Dedekind: the cubic field generated by a root of $x^3 - x^2 - 2x - 8$ is non-monogenic [3]. Even after this, Hasse's problem has been studied for a long time. Especially the research on monogenity of abelian extensions of the rational number field is classical. As mentioned above, it is known that a quadratic field K is monogenic, and we can write

$$K = \mathbb{Q}(\sqrt{d}), \qquad\qquad \mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & (d \equiv 2, 3 \bmod 4), \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & (d \equiv 1 \bmod 4) \end{cases}$$

with a square-free integer d. However, cyclic cubic fields are not always monogenic. G. Archinad [1] and M.-N. Gras [6, 7, 8] studied the monogenity of cyclic cubic fields independently. Especially Gras gave a necessary and sufficient condition for the monogenity as the existence of a suitable unit [7]. D. S. Dummit and H. Kisilevsky proved that there exist infinitely many monogenic and non-monogenic cyclic cubic fields [4]. Their method is the evaluation of inequalities using Baker's method. Let K be a cyclic extension over $\mathbb{Q}$ of prime degree $l \geq 5$. Gras showed that K is not monogenic unless K is the maximal real subfield of the cyclotomic field of prime conductor $2l + 1$ [6]. There are also some studies on a field whose degree is a composite number, for example [13, 14] by Nakahara. Recently, not only the monogenity of an algebraic number field K but also that of an extension of algebraic number field K/k with $k \supsetneq \mathbb{Q}$ has been studied. A power integral basis for K/k is called a *relative power integral basis*. For example, R. Schertz proved that ray class fields over an imaginary quadratic number field have a relative power integral basis over the Hilbert class field with some exceptions [17]. The methods that have been used in the research on power integral bases are analytical methods such as Baker's method and algebraic methods which are valid only under certain conditions. These methods can not be applied to general algebraic number fields, especially due to the difficulty that comes from growing degree. Therefore, we require a general method of determining power integral bases without depending on the degree and the application condition. The author has studied such a method from an algebraic perspective.

In the following we describe the main results. Let K be a cyclic cubic field and c_K be the conductor. We characterize cyclic cubic fields having power integral bases (Theorem 2.2.3). In this theorem, we use an integral ideal $\mathfrak{C}_K$ satisfying $N_{K/\mathbb{Q}}\mathfrak{C}_K = c_K$ and its principality. We give the equivalent conditions for when $\mathfrak{C}_K$ is principal (Theorem 2.3.1). From these two theorems, we obtain some concise and explicit equivalence conditions (Theorem 2.5.1). It is rather difficult to actually determine whether a cyclic cubic field has a power integral basis using the necessary and sufficient condition given by Gras, which is given in terms of the existence of a suitable unit. We obtain more explicit conditions. In addition, as one of the applications of the explicit condition, we can compute the power integral bases actually and summarize the results in the tables (Table 2.1, 2.2, and 2.3). These studies are the joint work with Tomokazu Kashio of Tokyo University of Science [11], and summarized in Chapter 2. A part of the results in this chapter can be derived also from the characterization by Gras. However our results have significance since our technique seems to be easier to generalize for the other settings. In fact, in Chapter 3, we introduce a generalization into the case of the relative cyclic extensions of prime degree.

Let l be an odd prime number and $k = \mathbb{Q}(\zeta + \zeta^{-1})$ where ζ is a primitive l-th root of unity. We provide a sufficient condition for the monogenity of relative cyclic extensions over k of degree l (Theorem 3.2.1). The condition is written explicitly with one parameter. If $l = 3$, then this condition is the necessary and sufficient condition and coincided with the condition given in Chapter 2. Using the explicit condition, we can investigate the monogenity and summarize the results for $l = 5$ in the table (Table 3.1). Furthermore, as an application of the condition, we prove that there exist infinitely many monogenic cyclic extensions over $\mathbb{Q}(\zeta + \zeta^{-1})$ for $l \geq 5$ (Theorem 3.5.1). The key to the proof is Shintani's fundamental domain, which enables us to reduce the problem of counting of ideals to that of elements. Previous researches suggest that a monogenic field is rare. For example, as mentioned above, Gras showed that the cyclic extensions over $\mathbb{Q}$ of degree $l \geq 5$ are non-monogenic with the exceptions of the maximal real subfields the cyclotomic fields. Our result means that we can construct the monogenic extensions of prime degree (≥ 5) infinitely by extending the base fields. The author believes that this phenomenon is interesting in comparison with the result of Gras. These studies are summarized in Chapter 3 and correspondent to the article [19].

Chapter 2

Cyclic cubic fields

The outline of this chapter is as follows. First, we introduce Shanks cubic polynomial $x^3 - tx^2 - (t+3)x - 1$ where t is a parameter in $\mathbb{Z}$. Next, we prove that if a cyclic cubic field K has a power integral basis, then K is a field generated by a root of Shanks cubic polynomial. Then, we characterize simplest cubic fields having a power integral basis and obtain the equivalent conditions for the monogenity of any cyclic cubic field. The main tools used in the proof are an integral ideal $\mathfrak{C}_K$ whose norm $N_{K/\mathbb{Q}}\mathfrak{C}_K$ is equal to the conductor c_K, Galois cohomology of the unit group, and Newton polygon of polynomials. As an application, we provide the tables summarizing the results of some calculations.

2.1 Shanks cubic polynomial

It is known that any cyclic cubic field is generated by a root of

$$f_t(x) := x^3 - tx^2 - (t+3)x - 1 \quad (t \in \mathbb{Q}).$$

In particular, if $t \in \mathbb{Z}$, $f_t(x)$ is called *Shanks cubic polynomial.* Let θ_t be a root of $f_t(x) = 0$ and put $K_t := \mathbb{Q}(\theta_t)$. In the following, we assume that $-1 \leqq t \in \mathbb{Z}$ since we have $K_t = K_{-(t+3)}$. We call a cyclic cubic field of the form K_t a *simplest cubic field.* The followings are well-known facts:

- $K_t/\mathbb{Q}$ is a cyclic cubic extension. We put

  $$G := \mathrm{Gal}(K_t/\mathbb{Q}) = \langle \sigma \rangle = \{\mathrm{id}, \sigma, \sigma^2\}.$$

- θ_t is a unit $\in \mathcal{O}_{K_t}^{\times}$ satisfying that (if necessary by replacing σ with σ^2)

  $$\sigma(\theta_t) = -\frac{1+\theta_t}{\theta_t}, \quad \sigma^2(\theta_t) = \frac{-1}{1+\theta_t}, \quad 1 + \theta_t + \theta_t\sigma(\theta_t) = 0, \quad N(\theta_t) = 1, \quad Tr(\theta_t) = t.$$

  We abbreviate as $N := N_{K/\mathbb{Q}}$, $Tr := Tr_{K/\mathbb{Q}}$.

- The discriminant of $f_t(X)$ is

  $$\prod_{0 \le i < j \le 2} (\sigma^i(\theta) - \sigma^j(\theta))^2 = (t^2 + 3t + 9)^2.$$

  We put $\Delta_t := t^2 + 3t + 9$.

- Let c_K and d_K denote the conductor and the discriminant, respectively. We have
$$c_{K_t} = \sqrt{d_{K_t}} \mid \Delta_t.$$
Here $a \mid b$ means that a divides b. The relation $c_K = \sqrt{d_K}$ follows from the conductor-discriminant formula.

We note that for a fixed K, there may exist more than one parameter t satisfying $K = K_t$. It is not easy to find all such parameters. However, by using some results on cubic Thue equations by Okazaki [15] and Hoshi [10, Theorem 1.4], we have $K_t \neq K_{t'}$ if $t \neq t'$ except for

$$K_{-1} = K_5 = K_{12} = K_{1259}, \qquad K_0 = K_3 = K_{54}, \qquad K_1 = K_{66}, \qquad K_2 = K_{2389}. \tag{2.1}$$

Note that $K_0 = K_3 = K_{54} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.

2.2 A characterization of monogenic cyclic cubic fields

The aim of this section is to provide a characterization of cyclic cubic fields having power integral bases (Theorem 2.2.3). Let $\mathfrak{C}_K$ be an integral ideal satisfying
$$N\mathfrak{C}_K = c_K.$$
Such a $\mathfrak{C}_K$ is determined uniquely. First we show that if K has a power integral basis, then we can write $\mathfrak{C}_K = (\alpha)$ with $Tr(\alpha) = 0$. More precisely we have the following.

Proposition 2.2.1. *Let K be a cyclic cubic field.*

(i) *There exists a unique integral ideal $\mathfrak{C}_K \subset \mathcal{O}_K$ satisfying $N\mathfrak{C}_K = c_K$.*

(ii) *The followings are equivalent for $\gamma \in \mathcal{O}_K$.*

(a) *γ is a generator of a power integral basis. That is, $\mathcal{O}_K = \mathbb{Z}[\gamma]$.*

(b) *$c_K = N(\gamma - \sigma(\gamma))$.*

(c) *$\mathfrak{C}_K = (\gamma - \sigma(\gamma))$.*

In particular, if K has a power integral basis, then $\mathfrak{C}_K$ is a principal ideal with a generator $\alpha := \gamma - \sigma(\gamma)$ satisfying $Tr(\alpha) = 0$.

Proof. (i) $p \mid c_K$ is equivalent to that p is (totally) ramified. In such a case, a unique prime ideal $\mathfrak{P}_p \mid p$ of $\mathcal{O}_K$ satisfies $N\mathfrak{P}_p = p$. Hence
$$\mathfrak{C}_K := \prod_{p \mid c_K} \mathfrak{P}_p^{v_p(c_K)}$$
is the unique ideal satisfying $N\mathfrak{C}_K = c_K$, where $v_p(n)$ denotes the order at a prime p of an integer n defined by
$$n = p^{v_p(n)} n_0, \quad (p, n_0) = 1.$$
(ii) We put $d(\gamma) := \prod_{\iota \neq \iota'} (\iota(\gamma) - \iota'(\gamma)) = N(\gamma - \sigma(\gamma))^2$, where ι, ι' run over all embeddings of K with $\iota \neq \iota'$. Then $\mathcal{O}_K = \mathbb{Z}[\gamma]$ means that $d_K = d(\gamma)$, which is equivalent to $c_K = N(\gamma - \sigma(\gamma))$. Then the assertion follows from (i). □

We consider the 1st cohomology group

$$H^1(G,\mathcal{O}_K^\times) = \left\{u \in \mathcal{O}_K^\times \mid N(u) = 1\right\} / \left\{u^{\sigma-1} \mid u \in \mathcal{O}_K^\times\right\}$$

and denote the class of $u \in \mathcal{O}_K^\times$ with $N(u) = 1$ by $[u] \in H^1(G,\mathcal{O}_K^\times)$. Then The following holds:

Lemma 2.2.2. *Let K be a cyclic cubic field. Assume that $\mathfrak{C}_K$ is principal, take a generator β of $\mathfrak{C}_K$, and put $u_\beta := \beta^{\sigma-1} \in \mathcal{O}_K^\times$. The followings are equivalent.*

(i) *There exists $\alpha \in \mathcal{O}_K$ satisfying $\mathfrak{C}_K = (\alpha)$, $Tr(\alpha) = 0$.*

(ii) *There exists $u \in \mathcal{O}_K^\times$ satisfying $1 + u + u\sigma(u) = 0$, $[u_\beta] = [u] \in H^1(G,\mathcal{O}_K^\times)$.*

(iii) *There exists t satisfying $K = K_t$, $[u_\beta] = [\theta_t] \in H^1(G,\mathcal{O}_K^\times)$.*

Proof. [(i) $\Leftrightarrow$ (ii)]. For any generator $\alpha := \beta\epsilon \in \mathfrak{C}_K$ ($\epsilon \in \mathcal{O}_K^\times$), we have

$$Tr(\alpha) = \beta\epsilon + \sigma(\beta\epsilon) + \sigma^2(\beta\epsilon) = \beta\epsilon(1 + u_\beta\epsilon^{\sigma-1} + u_\beta\epsilon^{\sigma-1}\sigma(u_\beta\epsilon^{\sigma-1})).$$

In particular, $Tr(\alpha) = 0$ is equivalent to $u := u_\beta\epsilon^{\sigma-1} \in [u_\beta]$ satisfying $1 + u + u\sigma(u) = 0$, as desired.

[(ii) $\Leftrightarrow$ (iii)]. ($\Leftarrow$) is obvious. For ($\Rightarrow$), we note that

if $1 + u + u\sigma(u) = 0$, then we have $0 = Tr(1 + u + u\sigma(u)) = 3 + Tr(u) + Tr(u\sigma(u))$.

On the other hand, by $u \in \mathcal{O}_K$, we have

$$t := Tr(u) \in \mathbb{Z}.$$

Therefore, u is a root of

$$(x - u)(x - \sigma(u))(x - \sigma^2(u)) = x^3 - Tr(u)x^2 + Tr(u\sigma(u))x - 1 = f_t(x).$$

Hence u is a conjugate $\tau(\theta_t)$ of θ_t ($\tau \in G$), so we have $u = \tau(\theta_t) = \theta_t(\theta_t)^{\tau-1} \in [\theta_t]$. □

By Proposition 2.2.1 and Lemma 2.2.2 we obtain the following (Theorem 2.2.3-(i)):

$$\text{If } K \text{ has a power integral basis, then } \begin{cases} K \text{ is a simplest cubic field,} \\ \mathfrak{C}_K \text{ is principal.} \end{cases}$$

However the "converse" does not hold true. We prepare some notations. For a number field k, we denote by I_k, P_k the group of all fractional ideals, all principal ideals, respectively. Additionally, we put

$$I_K^G := \{\mathfrak{A} \in I_K \mid \sigma(\mathfrak{A}) = \mathfrak{A}\}, \qquad P_K^G := I_K^G \cap P_K$$

to be the group of all ambiguous ideals, all principal ambiguous ideals, respectively. We easily see that

- $\mathfrak{C}_K \in I_K^G$. In particular, if $\mathfrak{C}_K$ is principal, then $\mathfrak{C}_K \in P_K^G$.

- Let $K = K_t$. Then $(\theta_t - \sigma(\theta_t)) \in P_K^G$.

In fact, by definition, we have $\sigma(\mathfrak{C}_K) = \mathfrak{C}_{\sigma(K)} = \mathfrak{C}_K$. The latter one follows from an explicit calculation:

$$\frac{\sigma(\theta_t) - \sigma^2(\theta_t)}{\theta_t - \sigma(\theta_t)} = \frac{-\frac{1+\theta_t}{\theta_t} - \frac{-1}{1+\theta_t}}{\theta_t + \frac{1+\theta_t}{\theta_t}} = \frac{-1}{1+\theta_t} = \sigma^2(\theta_t) \in \mathcal{O}_K^\times. \tag{2.2}$$

Additionally we consider the natural projection

$$P_K^G \to P_K^G/P_{\mathbb{Q}},\ \mathfrak{A} \mapsto \overline{\mathfrak{A}} := \mathfrak{A} \bmod P_{\mathbb{Q}}.$$

Then we can write a characterization of cyclic cubic fields having power integral bases as follows.

Theorem 2.2.3. *Let K be a cyclic cubic field.*

(i) *If K has a power integral basis, then we have*

- *K is a simplest cubic field.*
- *$\mathfrak{C}_K$ is principal.*

(ii) *Assume that K is a simplest cubic field and $\mathfrak{C}_K$ is principal, say $\mathfrak{C}_K = (\beta)$. The followings are equivalent.*

(a) *K has a power integral basis.*

(b) *There exists t satisfying that $K = K_t$ and $[\beta^{\sigma-1}] = [\theta_t] \in H^1(G, \mathcal{O}_K^\times)$.*

(c) *There exists t satisfying that $K = K_t$ and $\overline{\mathfrak{C}_K} = \overline{(\theta_t - \sigma(\theta_t))} \in P_K^G/P_{\mathbb{Q}}$.*

(d) *There exists t satisfying that $K = K_t$ and $\frac{\Delta_t}{c_K} \in \mathbb{N}^3 := \{n^3 \mid n \in \mathbb{N}\}$.*

Remark 2.2.4. *In* Theorem 2.2.3-(ii)*, $\beta^{\sigma-1} = \frac{\sigma(\beta)}{\beta} \in \mathcal{O}_K^\times$ since $\mathfrak{C}_K$ is an ambiguous ideal, and the cohomology class $[\beta^{\sigma-1}] \in H^1(G, \mathcal{O}_K^\times)$ does not depend on the choice of β since $[(\beta\epsilon)^{\sigma-1}] = [\beta^{\sigma-1}\epsilon^{\sigma-1}] = [\beta^{\sigma-1}]$ for $\epsilon \in \mathcal{O}_K^\times$.*

Proof of Theorem 2.2.3-(i). Let K be a cyclic cubic field with a generator γ of a power integral basis. Then $\mathfrak{C}_K$ is principal by Proposition 2.2.1. Moreover its generator $\alpha := \gamma - \sigma(\gamma)$ satisfies $Tr(\alpha) = 0$. It follows that K is a simplest cubic field by Lemma 2.2.2. □

We introduce the following proposition to prove Theorem 2.2.3-(ii).

Proposition 2.2.5. (i) *We have a canonical isomorphism*

$$P_K^G/P_{\mathbb{Q}} \cong H^1(G, \mathcal{O}_K^\times),\ \overline{(\alpha)} \mapsto [\alpha^{\sigma-1}].$$

(ii) *The norm map induces the following injective homomorphism*

$$I_K^G/P_{\mathbb{Q}} \hookrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^3,\ \overline{\mathfrak{A}} \mapsto N\mathfrak{A} \bmod (\mathbb{Q}^\times)^3.$$

In particular, we have

$$H^1(G, \mathcal{O}_K^\times) \cong P_K^G/P_{\mathbb{Q}} \subset I_K^G/P_{\mathbb{Q}} \hookrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^3.$$

Proof. (i) Consider the exact sequence

$$1 \to \mathcal{O}_K^\times \to K^\times \to P_K \to 1.$$

Then we have by Hilbert's Theorem 90

$$1 \to \{\pm 1\} \to \mathbb{Q}^\times \to P_K^G \to H^1(G, \mathcal{O}_K^\times) \to 1.$$

Hence we get

$$H^1(G, \mathcal{O}_K^\times) \cong [\mathrm{Coker}\colon \mathbb{Q}^\times \to P_K^G] = P_K^G/P_{\mathbb{Q}},\ [\alpha^{\sigma-1}] \leftarrow\!\shortmid \overline{(\alpha)}$$

by calculating the connecting homomorphism.

(ii) Since I_K^G is generated by ramified prime ideals and ideals contained in $P_{\mathbb{Q}}$, we can write any ideal contained in I_K^G as

$$\mathfrak{A} := (n) \prod_{p | c_K} \mathfrak{P}_p^{e_p} \text{ with } \mathfrak{P}_p^3 = (p),\ n \in \mathbb{N}.$$

Then we can write

$$N\mathfrak{A} = (n^3) \prod_{p | c_K} p^{e_p}.$$

Therefore $N\mathfrak{A} \in (\mathbb{Q}^\times)^3$ is equivalent to $e_p \in 3\mathbb{Z}$ for all p, which means $\mathfrak{A} \in P_{\mathbb{Q}}$. Hence the kernel of the norm map $I_K^G \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$ equals $P_{\mathbb{Q}}$. Then the assertion is clear. □

Proof of Theorem 2.2.3-(ii). Assume that K is a simplest cubic field and that $\mathfrak{C}_K = (\beta)$. The equivalences (b) ⇔ (c) ⇔ (d) follow from Proposition 2.2.5 by noting that

$$\begin{tikzcd}
H^1(G, \mathcal{O}_K^\times) \arrow[r, phantom, "\cong"] & P_K^G/P_{\mathbb{Q}} \arrow[r, hook] & \mathbb{Q}^\times/(\mathbb{Q}^\times)^3, \\
\rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} \\
{[u_\beta]} & \overline{\mathfrak{C}_K} \arrow[l, mapsto] \arrow[r, mapsto] & c_K \bmod (\mathbb{Q}^\times)^3, \\
{[\theta_t]} & \overline{(\theta_t - \sigma(\theta_t))} \arrow[l, mapsto] \arrow[r, mapsto] & \Delta_t \bmod (\mathbb{Q}^\times)^3.
\end{tikzcd}$$

Here, by (2.2), we obtain the bottom-left part as $[(\theta_t - \sigma(\theta_t))^{\sigma-1}] = [\sigma^2(\theta_t)] = [\theta_t \theta_t^{\sigma^2-1}] = [\theta_t] \in H^1(G, \mathcal{O}_K^\times)$. The part "(a) ⇒ (b)" follows by using Proposition 2.2.1-(ii)-[(a) ⇒ (c)] and Lemma 2.2.2-[(i) ⇒ (iii)] for $\alpha := \gamma - \sigma(\gamma)$. We prove the remaining part "(d) ⇒ (a)" by showing that a concrete element γ actually provides a power integral basis. We put

$$\gamma := \frac{\theta_t - a}{\sqrt[3]{\frac{\Delta_t}{c_K}}}$$

where $a \in \mathbb{Z}$. Then it suffices to show $\gamma \in \mathcal{O}_K$ for a suitable $a \in \mathbb{Z}$ since we have clearly $d(\gamma) = \frac{d(\theta_t)}{\left(\frac{\Delta_t}{c_K}\right)^2} = c_K^2 = d_K$. Since $(\theta_t - \sigma(\theta_t))$ is an ambiguous ideal, we see that $(\theta_t - \sigma(\theta_t))^3 = (N(\theta_t - \sigma(\theta_t)))$. On the other hand, we have $N(\theta_t - \sigma(\theta_t)) = \Delta_t \in c_K \cdot \mathbb{N}^3$. It follows that

$$\theta_t \equiv \sigma(\theta_t) \mod \sqrt[3]{\frac{\Delta_t}{c_K}}. \tag{2.3}$$

First assume $3 \nmid \sqrt[3]{\frac{\Delta_t}{c_K}}$. Then there exists $a \in \mathbb{Z}$ with $a \equiv \frac{t}{3} \bmod \sqrt[3]{\frac{\Delta_t}{c_K}}$ by $3 \in \left(\mathbb{Z}/\sqrt[3]{\frac{\Delta_t}{c_K}}\mathbb{Z}\right)^{\times}$, so we have

$$a \equiv \frac{t}{3} = \frac{Tr(\theta_t)}{3} \equiv \frac{3\theta_t}{3} = \theta_t \mod \sqrt[3]{\frac{\Delta_t}{c_K}}$$

by (2.3). Hence we have $\theta_t - a \in \sqrt[3]{\frac{\Delta_t}{c_K}}\mathcal{O}_K$, namely $\gamma = \frac{\theta_t - a}{\sqrt[3]{\frac{\Delta_t}{c_K}}} \in \mathcal{O}_K$. Next, assume $3 \mid \sqrt[3]{\frac{\Delta_t}{c_K}}$. Then we obtain $v_3(\Delta_t) = 3$, $3 \nmid c_K$, $v_3\left(\sqrt[3]{\frac{\Delta_t}{c_K}}\right) = 1$, $t \equiv 12 \bmod 27$ by Proposition 2.4.2. In this case, by (2.3), we have

$$t = Tr(\theta_t) \equiv 3\theta_t \mod \sqrt[3]{\frac{\Delta_t}{c_K}}.$$

It follows that

$$\theta_t - \frac{t}{3} \in \frac{1}{3}\sqrt[3]{\frac{\Delta_t}{c_K}}\mathcal{O}_K. \tag{2.4}$$

On the other hand, in Proof of Proposition 2.4.2-(iii) in §2.4, we show that $3 \mid \theta_t - \frac{t}{3}$ when $t \equiv 12 \bmod 27$. By combining this with (2.4), we obtain $\gamma = \frac{\theta_t - a}{\sqrt[3]{\frac{\Delta_t}{c_K}}} \in \mathcal{O}_K$ for $a = \frac{t}{3}$. □

Remark 2.2.6. *One of the key ideas is a relation between*

"power integral bases" and "units u satisfying $1 + u + u\sigma(u) = 0$":

There exists $\gamma \in \mathcal{O}_K$ satisfying $\mathcal{O}_K = \mathbb{Z}[\gamma]$ if and only if $\mathfrak{C}_K = (\gamma - \sigma(\gamma))$ (Proposition 2.2.1-(ii)-[(a) ⇔ (c)])*, and then $u := \frac{\sigma(\gamma-\sigma(\gamma))}{\gamma-\sigma(\gamma)}$ is a unit of K and satisfies $1 + u + u\sigma(u) = 0$ by* Lemma 2.2.2. *Note that the unit u is a root of Shanks cubic polynomial $f_t(X)$ with $t := Tr(u)$, namely $K = K_t$. It is known that Shanks cubic polynomial generates any cyclic cubic field. In* Chapter 3 *we consider the case where Shanks cubic polynomial is replaced by Rikuna's generic cyclic polynomial, which generates any cyclic extension over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ with $\zeta_n := e^{\frac{2\pi i}{n}}$. We expect to get new results in other cases, for example other generic polynomials. Besides, in* [5]*, elements u satisfying*

$$1 + u + u\sigma(u) + \cdots + u\sigma(u)\cdots\sigma^{n-2}(u) = 0,$$

are studies in terms of "simplest" number fields, and Hilbert's Theorem 90. *The relation to the technique in this paper also seems to be interesting.*

2.3 Equivalent conditions for the principality of $\mathfrak{C}_{K_t}$

For many simplest cubic fields K_t, we can observe that if $\mathfrak{C}_K$ is principal, then K_t is monogenic (note that there are counterexamples (Section 2.6)). Thus we focus on when $\mathfrak{C}_{K_t}$ is principal. The aim of this section is to provide the equivalent conditions (Theorem 2.3.1 and Corollary 2.3.4).

Theorem 2.3.1. *Let $K = K_t$. For simplicity, assume that $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. The followings are equivalent.*

(i) *$\mathfrak{C}_K$ is principal.*

(ii) *$\overline{\mathfrak{C}_K} = \overline{(\theta_t - \sigma(\theta_t))}$ or $\overline{(\theta_t - \sigma(\theta_t))^2} \in P_K^G/P_{\mathbb{Q}}$.*

(iii) *$\frac{\Delta_t}{c_K}$ or $\frac{\Delta_t^2}{c_K} \in \mathbb{N}^3$.*

Remark 2.3.2. *The condition of* Theorem 2.3.1-(i) *is independent of the choice of t with $K = K_t$, so are those of* Theorem 2.3.1-(ii), (iii). *We also note that the exception $\mathfrak{C}_{\mathbb{Q}(\zeta_9+\zeta_9^{-1})}$ is a principal ideal $(= (\zeta_9 + \zeta_9^{-1} + 1)^2)$.*

We prepare some notations and properties to prove Theorem 2.3.1. Let $K = K_t$ be a simplest cubic field generated by a root θ_t of $f_t(x)$. Recall that

- The ambiguous ideal $\mathfrak{C}_K$ satisfies $N\mathfrak{C}_K = c_K$.
- The principal ambiguous ideal $(\theta_t - \sigma(\theta_t))$ satisfies $N(\theta_t - \sigma(\theta_t)) = \Delta_t$.
- We have a diagram

$$\begin{tikzcd}
H^1(G, \mathcal{O}_K^\times) \arrow[r, phantom, "\cong"] & P_K^G/P_{\mathbb{Q}} \arrow[r, phantom, "\subset"] & I_K^G/P_{\mathbb{Q}} \arrow[r, hook] & \mathbb{Q}^\times/(\mathbb{Q}^\times)^3, \\
\cup & \cup & \cup & \\
 & & \overline{\mathfrak{C}_K} \arrow[r, mapsto] & c_K \bmod (\mathbb{Q}^\times)^3, \\
{[\theta_t]} & \overline{(\theta_t - \sigma(\theta_t))} \arrow[l, mapsto] \arrow[rr, mapsto] & & \Delta_t \bmod (\mathbb{Q}^\times)^3
\end{tikzcd} \tag{2.5}$$

  without assuming that $\mathfrak{C}_K$ is principal, by Proposition 2.2.5 and Proof of Theorem 2.2.3-(ii) in the previous section.

Proposition 2.3.3. *Let K be a cyclic cubic field. We have*

$$H^1(G, \mathcal{O}_K^\times) \cong \mathbb{Z}/3\mathbb{Z}.$$

Proof. For a finite cyclic extension L/F, the Herbrand quotient $Q(\mathcal{O}_L^\times)$ equals $\frac{1}{[L:F]}\times$ "the product of ramification indices of all the infinite places" (for a proof, see [22, Lemma 3]). Therefore we see that

$$\frac{1}{|H^1(G, \mathcal{O}_K^\times)|} = Q(\mathcal{O}_K^\times) = \frac{1}{3},$$

since $N\colon \mathcal{O}_K^\times \to \mathbb{Z}^\times$ is surjective. Then the assertion is clear. □

Proof of Theorem 2.3.1. Let $K = K_t \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. First we show that $(\theta_t - \sigma(\theta_t)) \notin P_{\mathbb{Q}}$ (strictly speaking, $(\theta_t - \sigma(\theta_t)) \notin [\mathrm{Im}\colon P_{\mathbb{Q}} \hookrightarrow P_K^G]$). If $(\theta_t - \sigma(\theta_t)) \in P_{\mathbb{Q}}$, then $N(\theta_t - \sigma(\theta_t)) = \Delta_t \in \mathbb{N}^3$, which implies that $p \nmid c_K$ for any $p \neq 3$ by Proposition 2.4.3. It contradicts with $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. We see also that $\mathfrak{C}_K \notin P_{\mathbb{Q}}$ by Proposition 2.4.1. Then we can write by (2.5) and Proposition 2.3.3

$$\begin{tikzcd}
P_K^G/P_{\mathbb{Q}} \arrow[r, phantom, "\subset"] & I_K^G/P_{\mathbb{Q}} \arrow[r, hook] & \mathbb{Q}^\times/(\mathbb{Q}^\times)^3, \\
\parallel & \cup & \\
\left\{\overline{(\theta_t - \sigma(\theta_t))}^e \mid e = 0, 1, 2\right\} & \overline{\mathfrak{C}_K} \neq \overline{(1)}. &
\end{tikzcd}$$

Therefore $\overline{\mathfrak{C}_K} \in P_K^G/P_{\mathbb{Q}}$ (namely, that $\mathfrak{C}_K$ is principal) is equivalent to each of the following statements:

- There exists $e \in \{1,2\}$ satisfying $\mathfrak{C}_K \equiv (\theta_t - \sigma(\theta_t))^e \bmod P_{\mathbb{Q}}$.
- There exists $e \in \{1,2\}$ satisfying $c_K \equiv \Delta_t^e \bmod (\mathbb{Q}^\times)^3$.

Then the assertion is clear. □

We also provide an explicit version of Theorem 2.3.1 whose conditions are written explicitly in terms of t.

Corollary 2.3.4. *Let $K = K_t \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. The followings are equivalent.*

(i) *$\mathfrak{C}_K$ is principal.*

(ii) $$\begin{cases} v_p(\Delta_t) \equiv 1 \bmod 3 \textit{ for all } p \mid c_K \textit{ or } v_p(\Delta_t) \equiv 2 \bmod 3 \textit{ for all } p \mid c_K & (3 \nmid c_K), \\ v_3(\Delta_t) = 2,\ v_p(\Delta_t) \equiv 1 \bmod 3 \textit{ for all } 3 \neq p \mid c_K & (3 \mid c_K). \end{cases}$$

(iii) $$\begin{cases} v_p(\Delta_t) \not\equiv 1 \bmod 3 \textit{ for all } p \textit{ or } v_p(\Delta_t) \not\equiv 2 \bmod 3 \textit{ for all } p & \\ & (3 \nmid t \textit{ or } t \equiv 12 \bmod 27), \\ v_p(\Delta_t) \not\equiv 2 \bmod 3 \textit{ for all } p \neq 3 & (t \equiv 0, 6 \bmod 9). \end{cases}$$

Proof. The equivalence (ii) ⇔ (iii) follows from Propositions 2.4.2, 2.4.3 immediately. We prove "(i) ⇔ (ii)". By Propositions 2.4.1, 2.4.2, 2.4.3, we see that

- When $p \neq 3$ we have
$$v_p(c_{K_t}) = 0, 1, \qquad v_p(c_{K_t}) = 0 \Leftrightarrow v_p(\Delta_t) \equiv 0 \bmod 3.$$
- For $p = 3$ we have
$$v_3(\Delta_t) = 0, 2, 3, \quad 3 \nmid c_{K_t} \Rightarrow v_3(\Delta_t) = 0, 3, \quad 3 \mid c_{K_t} \Leftrightarrow 3^2 \| c_{K_t} \Rightarrow v_3(\Delta_t) = 2, 3.$$

By Theorem 2.3.1, $\mathfrak{C}_K$ is principal if and only if

$$e = 1 \text{ or } 2 \text{ satisfies } v_p(\Delta_t) \equiv e v_p(c_K) \bmod 3 \text{ for all } p. \tag{2.6}$$

When $3 \nmid c_K$, we may rewrite (2.6) as

$$e = 1 \text{ or } 2 \text{ satisfies } v_p(\Delta_t) \equiv e v_p(c_K) \bmod 3 \text{ for all } p \mid c_K$$

and

$$e = 1 \text{ or } 2 \text{ satisfies } v_p(\Delta_t) \equiv e \bmod 3 \text{ for all } p \mid c_K \text{ (that is, (ii) with } 3 \nmid c_K)$$

by using the facts that

$$\begin{aligned} v_p(c_K) &= 0 \equiv e v_p(\Delta_t) \quad \bmod 3 && (p \nmid c_K), \\ v_p(c_K) &= 1 && (p \mid c_K) \end{aligned}$$

respectively.

When $3 \mid c_K$, we have $v_3(\Delta_t) \not\equiv 2v_3(c_K) \bmod 3$ by $v_3(\Delta_t) = 2, 3$, $v_3(c_K) = 2$. Hence (2.6) can be rewrite as

$$v_p(\Delta_t) \equiv v_p(c_K) \bmod 3 \text{ for all } p \mid c_K$$

since the case of $e = 2$ in (2.6) can not happen. This is equivalent to

$$v_3(\Delta_t) = 2, \qquad\qquad v_p(\Delta_t) \equiv 1 \bmod 3 \text{ for all } 3 \neq p \mid c_K$$

(that is (ii) with $3 \mid c_K$) by $v_3(\Delta_t) = 2, 3$, $v_3(c_K) = 2$, and $v_p(c_K) = 1$ ($3 \neq p \mid c_K$). Then the assertion is clear. □

2.4 Primes dividing c_K, Δ_t

In this section, we recall properties of primes dividing c_K or Δ_t used in the proof above. First we note that

$$\{\text{all the ramified primes}\} = \{\text{all the primes dividing } c_{K_t}\} \subset \{\text{all the primes dividing } \Delta_t\}$$

since $c_{K_t} \mid \Delta_t$. The following propositions are well-known for experts.

Proposition 2.4.1. *Let K be a cyclic cubic field and p be a prime number. The conductor c_K satisfies the following conditions.*

(i) *If $3 \mid c_K$, then $v_3(c_K) = 2$.*

(ii) *If $p \equiv 1 \bmod 3$, then $p \mid c_K$ implies $v_p(c_K) = 1$.*

(iii) *If $p \equiv 2 \bmod 3$, then $p \nmid c_K$.*

Proposition 2.4.2. *Let $K = K_t$. Then $v_3(\Delta_t)$ takes only values of $0, 2, 3$. More precisely, we have the following.*

(i) *$v_3(\Delta_t) = 0$ if and only if $3 \nmid t$. In this case, $3 \nmid c_K$.*

(ii) *$v_3(\Delta_t) = 2$ if and only if $t \equiv 0, 6 \bmod 9$. In this case, $3 \mid c_K$.*

(iii) *$v_3(\Delta_t) = 3$ if and only if $t \equiv 3 \bmod 9$. In this case,*

$$\begin{cases} t \equiv 12 \bmod 27 & \textit{is equivalent to } 3 \nmid c_K, \\ t \equiv 3, 21 \bmod 27 & \textit{is equivalent to } 3 \mid c_K. \end{cases}$$

In particular, we have that

$$\begin{cases} 3 \nmid c_K & \textit{is equivalent to } 3 \nmid t \textit{ or } t \equiv 12 \bmod 27, \\ 3 \mid c_K & \textit{is equivalent to } t \equiv 0, 6 \bmod 9 \textit{ or } t \equiv 3, 21 \bmod 27. \end{cases} \tag{2.7}$$

Proposition 2.4.3. *Let $K = K_t$, $p \neq 3$. The followings are equivalent.*

$$v_p(\Delta_t) \equiv 0 \bmod 3 \textit{ is equivalent to } p \nmid c_K.$$

Proposition 2.4.1 can be shown by noting that c_K is the minimal integer satisfying $K_t \subset \mathbb{Q}(\zeta_{c_K})$, which implies

$$\prod_{p \mid c_K} (\mathbb{Z}/p^{v_p(c_K)}\mathbb{Z})^\times \cong (\mathbb{Z}/c_K\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{c_K})/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(K/\mathbb{Q})) \cong \mathbb{Z}/3\mathbb{Z}.$$

Here, we give a proof only of Proposition 2.4.2 since that of Proposition 2.4.3 is similar and simpler.

Proof of Proposition 2.4.2. The "if and only if" part follows from an explicit calculation as

$$\begin{aligned} \Delta_{3t_0} &= 9t_0^2 + 9t_0 + 9, & \Delta_{3t_0+1} &= 9t_0^2 + 15t_0 + 13, & \Delta_{3t_0+2} &= 9t_0^2 + 21t_0 + 19, \\ \Delta_{9t_0} &= 9(9t_0^2 + 3t_0 + 1), & \Delta_{9t_0+3} &= 27(3t_0^2 + 3t_0 + 1), & \Delta_{9t_0+6} &= 9(9t_0^2 + 15t_0 + 7). \end{aligned}$$

Then (i) holds true since $c_K \mid \Delta_t$.
(ii) Let $t = 9t_0$. Then the minimal polynomial of $\theta_t - \frac{t}{3} - 1$:

$$x^3 + 3x^2 + (-27t_0^2 - 9t_0)x + (-54t_0^3 - 54t_0^2 - 18t_0 - 3)$$

is an Eisenstein polynomial, so we have $3 \mid c_K$. Similarly, let $t = 9t_0 + 6$. Then the minimal polynomial of $\theta_t - \frac{t}{3} + 1$:

$$x^3 - 3x^2 + (-27t_0^2 - 45t_0 - 18)x + (-54t_0^3 - 108t_0^2 - 72t_0 - 15)$$

also is an Eisenstein polynomial, so we have $3 \mid c_K$.
(iii) Assume $t \equiv 3 \bmod 9$. Then the minimal polynomial of $\theta_t - \frac{t}{3}$ is

$$x^3 - \frac{\Delta_t}{3}x - \frac{(2t+3)\Delta_t}{3^3} \in \mathbb{Z}[x].$$

Here we note that $v_3(\Delta_t) = 3$. First assume that $t \equiv 3, 21 \bmod 27$, which implies $v_3(2t + 3) = 2$. Then the Newton polygon is given by

$$v_3(1) = 0, \qquad v_3(0) = \infty, \qquad v_3(\tfrac{\Delta_t}{3}) = 2, \qquad v_3(\tfrac{(2t+3)\Delta_t}{3^3}) = 2,$$

so we have $v_3(\theta_t - \frac{t}{3}) = \frac{2}{3}$. That is, 3 ramifies in $K_t = \mathbb{Q}(\theta_t - \frac{t}{3})$. Next assume that $t \equiv 12 \bmod 27$, which implies $v_3(2t + 3) \geqq 3$. In this case, the Newton polygon is given by

$$v_3(1) = 0, \qquad v_3(0) = \infty, \qquad v_3(\tfrac{\Delta_t}{3}) = 2, \qquad v_3(\tfrac{(2t+3)\Delta_t}{27}) \geqq 3.$$

That is, $3 \mid \theta_t - \frac{t}{3}$. Then the discriminant of (the minimal polynomial of) $\frac{\theta_t - \frac{t}{3}}{3}$ equals $(\frac{\Delta_t}{3^3})^2$, which is prime to 3. Note that $c_K \mid \frac{\Delta_t}{3^3}$ since $\mathbb{Z}\left[\frac{\theta_t - \frac{t}{3}}{3}\right] \subset \mathcal{O}_{K_t}$. Then we obtain $3 \nmid c_K$ as desired. □

Finally in this section, we derive the characterization

$$c_{K_t} = \begin{cases} \prod\limits_{v_p(\Delta_t) \not\equiv 0 \bmod 3} p & (3 \nmid t \text{ or } t \equiv 12 \bmod 27), \\ 3^2 \prod\limits_{p \neq 3, v_p(\Delta_t) \not\equiv 0 \bmod 3} p & (\text{otherwise}). \end{cases} \tag{2.8}$$

The division into two cases comes from whether $3 \mid c_{K_t}$ or not, by Proposition 2.4.2. The range of p and its exponent follow from Proposition 2.4.3 and Proposition 2.4.1, respectively.

2.5 Explicit equivalent conditions for the monogenity

We provide more explicit equivalent conditions for the monogenity of the ring of integers of any cyclic cubic field (Theorem 2.5.1 and Corollary 2.5.3).

Theorem 2.5.1. *Let K be a cyclic cubic field. The followings are equivalent.*

(i) *K has a power integral basis.*

(ii) *There exists t satisfying that $K = K_t$ and*

$$\frac{\Delta_t}{c_K} \in \mathbb{N}^3 = \left\{ n^3 \mid n \in \mathbb{N} \right\}. \tag{2.9}$$

(iii) *There exists t satisfying that $K = K_t$ and*

$$t \not\equiv 3, 21 \bmod 27, \qquad v_p(\Delta_t) \not\equiv 2 \bmod 3 \textit{ for all } p \neq 3. \tag{2.10}$$

In such a case, a power integral basis $\gamma \in \mathcal{O}_K$ is given by

$$\gamma := \frac{\theta_t - a}{\sqrt[3]{\frac{\Delta_t}{c_K}}} \textit{ for } a \in \mathbb{Z} \textit{ with } a \equiv \frac{t}{3} \bmod \sqrt[3]{\frac{\Delta_t}{c_K}}. \tag{2.11}$$

Remark 2.5.2. *The condition $a \equiv \frac{t}{3} \bmod \sqrt[3]{\frac{\Delta_t}{c_K}}$ in* (2.11) *means the following. We have $3 \mid t$ when $3 \mid \sqrt[3]{\frac{\Delta_t}{c_K}}$ by* Proposition 2.4.2-(i)*. Hence, strictly speaking, we take an integer a satisfying*

$$\begin{cases} a \equiv \dfrac{t}{3} \bmod \sqrt[3]{\frac{\Delta_t}{c_K}} & \left(3 \mid \sqrt[3]{\frac{\Delta_t}{c_K}}\right), \\ 3a \equiv t \bmod \sqrt[3]{\frac{\Delta_t}{c_K}} & \left(3 \nmid \sqrt[3]{\frac{\Delta_t}{c_K}}\right). \end{cases}$$

Proof. The expression (2.11) of a power integral basis is given in the proof of Theorem 2.2.3-[(d) ⇒ (a)]. We show that the following conditions in Theorem 2.5.1 are equivalent (we rewrite ⓘⓘⓘ slightly by using Proposition 2.4.2):

$\textcircled{i}$ K has a power integral basis.

$\textcircled{ii}$ There exists t satisfying that $K = K_t$ and $\frac{\Delta_t}{c_K} \in \mathbb{N}^3$.

$\textcircled{iii}$ There exists t satisfying that $K = K_t$ and

$$\begin{cases} v_p(\Delta_t) \not\equiv 2 \bmod 3 \text{ for all } p & (3 \nmid t \text{ or } t \equiv 12 \bmod 27), \\ v_p(\Delta_t) \not\equiv 2 \bmod 3 \text{ for all } p \neq 3 & (t \equiv 0, 6 \bmod 9). \end{cases}$$

The equivalence $\textcircled{i} \Leftrightarrow \textcircled{ii}$ follows from Theorem 2.2.3-(i), Theorem 2.2.3-(ii)-[(a) $\Leftrightarrow$ (d)] and Theorem 2.3.1-[(i) $\Leftrightarrow$ (iii)] immediately. Hence it suffices to show that $\textcircled{i}$ & $\textcircled{ii} \Rightarrow \textcircled{iii} \Rightarrow \textcircled{ii}$. When $K = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, the assertion holds since $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ satisfies both of $\textcircled{ii}$, $\textcircled{iii}$ by $\mathbb{Q}(\zeta_9 + \zeta_9^{-1}) = K_0$, $c_{\mathbb{Q}(\zeta_9 + \zeta_9^{-1})} = \Delta_0 = 9$. We assume that $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.

[$\textcircled{i}$ & $\textcircled{ii} \Rightarrow \textcircled{iii}$]. Assume that $\textcircled{i}$ holds. Then $\mathfrak{C}_K$ is principal by Theorem 2.2.3-(i). There are three cases by Corollary 2.3.4-[(i) $\Leftrightarrow$ (iii)]:

(a) $v_p(\Delta_t) \not\equiv 1 \bmod 3$ for all p and ($3 \nmid t$ or $t \equiv 12 \bmod 27$).

(b) $v_p(\Delta_t) \not\equiv 2 \bmod 3$ for all p and ($3 \nmid t$ or $t \equiv 12 \bmod 27$).

(c) $v_p(\Delta_t) \not\equiv 2 \bmod 3$ for all $p \neq 3$ and ($t \equiv 0, 6 \bmod 9$).

Note that $\textcircled{iii}$ states that only (b) or (c) holds. On the other hand, $\textcircled{ii}$ states that

$$v_p(\Delta_t) \equiv v_p(c_K) \bmod 3 \text{ for all } p. \tag{2.12}$$

Since $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, there exists $p \mid c_K, \neq 3$, which satisfies

$$v_p(c_K) = 1 \tag{2.13}$$

by Proposition 2.4.1. Hence (a) and (2.12) do not hold simultaneously.

[$\textcircled{iii} \Rightarrow \textcircled{ii}$]. Assume $\textcircled{iii}$ holds. Then $\mathfrak{C}_K$ is principal since $\textcircled{iii}$ is a part of the condition of Corollary 2.3.4-(iii). Therefore we have $\frac{\Delta_t}{c_K}$ or $\frac{\Delta_t^2}{c_K} \in \mathbb{N}^3$ by Theorem 2.3.1. However, under $\textcircled{iii}$, $\frac{\Delta_t^2}{c_K} \in \mathbb{N}^3$ can not hold by (2.13). Then the assertion is clear. □

As mentioned in Section 2.1, there may exist more than one parameter t satisfying $K = K_t$ for a fixed K. For example, let $K := \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Then $K = K_0 = K_3$. Although a parameter $t = 3$ does not satisfy (2.9) (and (2.10)), K has a power integral basis since another parameter $t = 0$ satisfies it. Namely, Theorem 2.5.1 "practically" provides only sufficient condition for monogenity of K. However, all such parameters are known. We recall (2.1):

$$K_{-1} = K_5 = K_{12} = K_{1259}, \quad K_0 = K_3 = K_{54} (= \mathbb{Q}(\zeta_9 + \zeta_9^{-1})), \quad K_1 = K_{66}, \quad K_2 = K_{2389}.$$

We see that the parameters $t = -1, 0, 1, 2$ satisfy (2.9) (for Δ_t and c_K, see Table 2.1) and (2.10). Hence we obtain the following explicit equivalent condition.

Corollary 2.5.3. *If a cyclic cubic field K has a power integral basis, then it is a simplest cubic field, that is, there exists t satisfying that $K = K_t$. Moreover, the following are equivalent.*

(i) *K_t has a power integral basis.*

(ii) $t \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ *or t satisfies that* $\frac{\Delta_t}{c_{K_t}} \in \mathbb{N}^3$.

(iii) $t \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ *or t satisfies that* $t \not\equiv 3, 21 \bmod 27$ *and that* $v_p(\Delta_t) \not\equiv 2 \bmod 3$ *for all* $p \neq 3$.

In such a case, a power integral basis is given by (2.11).

Remark 2.5.4. *The condition in* Theorem 2.5.1-(iii) *or* Corollary 2.5.3-(iii) *is given in terms of t (note that $\Delta_t = t^2 + 3t + 9$). Namely, we can determine the monogenity only by the parameter t, without studying the number field K_t itself. For example, K_4 is monogenic since* $4 \not\equiv 3, 21 \bmod 27$ *and* $\Delta_4 = 37$.

Remark 2.5.5. (i) *Our basic idea is to decompose the monogenity of K into two steps:*

- *$\mathfrak{C}_K$ is principal where one of its generator α satisfying $Tr(\alpha) = 0$.*
- *There exists $\gamma \in \mathcal{O}_K$ satisfying $\alpha = \gamma - \sigma(\gamma)$ (i.e, a special case of the integral version of additive Hilbert's Theorem 90), which have to provide a power integral basis of K.*

This idea was established in [18].

(ii) *Some arguments in this chapter can be seen also in* [2]. *Moreover,* [2, Lemma 1] *states that if Δ_t is square-free, then K_t has a power integral basis. This is a special case of* Theorem 2.5.1-[(iii) $\Rightarrow$ (i)].

(iii) *An large part of the equivalent condition is covered by the classical one of Gras. However we write the condition more explicitly. Let K be a cyclic cubic field. Gras* [6, Théorème 2] *showed that the followings are equivalent.*

(a) *K has a power integral basis.*

(b) *There exists a unit $u \in \mathcal{O}_K^\times$ satisfying*

$$N(u) = 1, \qquad Tr(u + u^{-1}) + 3 = 0, \qquad Tr\left(\frac{u^2 - u^{-1}}{c_K}\right) \in \mathbb{N}^3.$$

This corresponds to Theorem 2.5.1-[(i) $\Leftrightarrow$ (ii)] *in this chapter and we provide an alternative proof. In fact, $N(u) = 1$ and $Tr(u+u^{-1})+3 = 0$ imply $Tr(u)+Tr(uu')+3 = 0$ where u' is a conjugate of u. It follows that u is a root of $f_t(x)$ with $t := Tr(u)$, that is, $K = K_t$. Then we see that $Tr(u^2 - u^{-1}) = Tr(u)^2 - 3\,Tr(uu') = t^2 + 3t + 9$.*

2.6 Examples

Table 2.1 below is a list of t, the prime factorization of c_{K_t} (the ramified primes), the prime factorization of Δ_t, the corresponding "case", and the other t' satisfying $K_t = K_{t'}$. There are 3 "cases":

(a) K_t has a power integral basis by Theorem 2.5.1 (or Corollary 2.5.3).

(b) K_t has a power integral basis since another t' with $K_t = K_{t'}$ satisfies (2.9) and (2.10) although t does not satisfy them.

(c) K_t does not have a power integral basis by Corollary 2.5.3.

For example,

- K_{-1}, K_0, K_1, K_2 have power integral bases since $t = -1, 0, 1, 2$ satisfy (2.9) and (2.10).
- K_3 has a power integral basis since $K_3 = K_0$ although $t = 3$ does not satisfy (2.9) and (2.10).
- K_{21} is the first example which does not have a power integral basis by Corollary 2.5.3.

Table 2.2 below is a list of K_t which do <u>*not*</u> have power integral bases up to $t = 2000$.

Table 2.3 below is a list of "non-trivial cases" which satisfy $\mathcal{O}_{K_t} \supsetneqq \mathbb{Z}[\theta_t]$ and $\mathfrak{C}_{K_t}$ is principal. Note that

- When $\mathcal{O}_{K_t} = \mathbb{Z}[\theta_t]$ (that is $c_{K_t} = \Delta_t$), it has a (trivial) generator θ_t of a power integral basis.
- When $\mathfrak{C}_{K_t}$ is not principal, it does not have a power integral basis by Theorem 2.2.3.
- If $t < 101471$, then the converse of Theorem 2.2.3-(i): "$\mathfrak{C}_{K_t}$ is principal $\Rightarrow$ K_t has a power integral basis" also holds true. All the examples of

  "$\mathfrak{C}_{K_t}$ is principal but K_t does not have a power integral basis"
  up to $t = 10^8 = 100000000$

  are $t = 101471, 182451, 18128865$.
- K_{740} has a power integral basis although $v_7(\Delta_{740}) = 4 \neq 1$. This is the first example of "K_t has a power integral basis although the prime-to-3 part of Δ_t is not square-free" (cf. Cusick's result in Remark 2.5.5-(ii)), except for the exceptions K_5 $(= K_{-1})$, K_{54} $(= K_0)$, K_{66} $(= K_1)$.

t	c_{K_t}			Δ_t			case	$= K_{t'}$
-1	7			7^1			(a)	5,12,1259
0	3^2			3^2			(a)	3,54
1	13			13^1			(a)	66
2	19			19^1			(a)	2389
3	3^2			3^3			(b)	0,54
4	37			37^1			(a)	
5	7			7^2			(b)	-1,12,1259
6	3^2	7		3^2	7^1		(a)	
7	79			79^1			(a)	
8	97			97^1			(a)	
9	3^2	13		3^2	13^1		(a)	
10	139			139^1			(a)	
11	163			163^1			(a)	
12	7			3^3	7^1		(a)	-1,5,1259
13	7	31		7^1	31^1		(a)	
14	13	19		13^1	19^1		(a)	
15	3^2	31		3^2	31^1		(a)	
16	313			313^1			(a)	
17	349			349^1			(a)	
18	3^2	43		3^2	43^1		(a)	
19	7	61		7^1	61^1		(a)	
20	7	67		7^1	67^1		(a)	
21	3^2	19		3^3	19^1		(c)	
22	13	43		13^1	43^1		(a)	
23	607			607^1			(a)	
24	3^2	73		3^2	73^1		(a)	
25	709			709^1			(a)	
26	7	109		7^1	109^1		(a)	
27	3^2	7	13	3^2	7^1	13^1	(a)	
28	877			877^1			(a)	
29	937			937^1			(a)	
30	3^2	37		3^3	37^1		(c)	

Table 2.1: small t

K_t $(-1 \leqq t \leqq 2000)$ of case (c)
21, 30, 41, 48, 57, 75, 84, 90, 100, 102, 103, 111,
129, 138, 139, 152, 154, 156, 165, 183, 188, 192,
201, 204, 210, 219, 235, 237, 246, 250, 264, 269,
271, 273, 291, 299, 300, 318, 327, 335, 345, 348,
354, 356, 372, 374, 381, 384, 398, 399, 404, 408,
426, 433, 435, 438, 446, 453, 462, 480, 482, 489,
495, 507, 515, 516, 531, 534, 543, 544, 561, 565,
570, 573, 577, 580, 588, 593, 597, 602, 607, 615,
624, 642, 651, 669, 678, 691, 696, 705, 716, 723,
727, 732, 742, 750, 759, 776, 777, 786, 789, 804,
813, 825, 831, 838, 840, 844, 858, 867, 874, 876,
885, 887, 894, 912, 921, 923, 926, 936, 939, 945,
948, 966, 975, 985, 992, 993, 1002, 1020, 1021,
1029, 1034, 1047, 1056, 1070, 1074, 1080, 1083,
1096, 1101, 1110, 1114, 1119, 1128, 1132, 1137,
1155, 1164, 1168, 1181, 1182, 1191, 1209, 1210,
1217, 1218, 1230, 1236, 1237, 1245, 1249, 1263,
1265, 1266, 1269, 1272, 1279, 1287, 1290, 1299,
1317, 1326, 1328, 1344, 1353, 1364, 1371, 1377,
1380, 1398, 1407, 1413, 1418, 1425, 1434, 1452,
1461, 1462, 1475, 1479, 1488, 1497, 1506, 1511,
1515, 1524, 1533, 1542, 1560, 1563, 1569, 1573,
1587, 1596, 1609, 1614, 1621, 1622, 1623, 1641,
1648, 1650, 1668, 1671, 1677, 1695, 1704, 1707,
1720, 1722, 1731, 1743, 1749, 1756, 1758, 1776,
1785, 1790, 1803, 1805, 1812, 1818, 1830, 1839,
1854, 1857, 1866, 1867, 1884, 1893, 1903, 1911,
1916, 1920, 1925, 1938, 1947, 1952, 1959, 1965,
1974, 1992

Table 2.2: non-monogenic t

t	c_{K_t}			Δ_t					case	$= K_{t'}$
3	3^2			3^3					(b)	0,54
5	7			7^2					(b)	-1,12,1259
12	7			3^3	7^1				(a)	-1,5,1259
39	61			3^3	61^1				(a)	
54	3^2			3^2	7^3				(a)	0,3
66	13			3^3	13^2				(b)	1
93	331			3^3	331^1				(a)	
120	547			3^3	547^1				(a)	
147	19	43		3^3	19^1	43^1			(a)	
174	7	163		3^3	7^1	163^1			(a)	
228	1951			3^3	1951^1				(a)	
255	2437			3^3	2437^1				(a)	
282	13	229		3^3	13^1	229^1			(a)	
286	241			7^3	241^1				(a)	
309	3571			3^3	3571^1				(a)	
336	4219			3^3	4219^1				(a)	
363	7	19	37	3^3	7^1	19^1	37^1		(a)	
390	7	811		3^3	7^1	811^1			(a)	
397	463			7^3	463^1				(a)	
417	13	499		3^3	13^1	499^1			(a)	
444	7351			3^3	7351^1				(a)	
471	8269			3^3	8269^1				(a)	
498	9241			3^3	9241^1				(a)	
525	10267			3^3	10267^1				(a)	
552	7	1621		3^3	7^1	1621^1			(a)	
579	7	1783		3^3	7^1	1783^1			(a)	
606	13669			3^3	13669^1				(a)	
629	19	61		7^3	19^1	61^1			(a)	
633	13	31	37	3^3	13^1	31^1	37^1		(a)	
660	19	853		3^3	19^1	853^1			(a)	
687	97	181		3^3	97^1	181^1			(a)	
714	67	283		3^3	67^1	283^1			(a)	
740	7	229		7^4	229^1				(a)	
101471	5479			7^3	5479^2				(c)	
182451	13	37	73	3^3	13^2	37^2	73^2		(c)	
18128865	13	43	337	3^3	7^3	13^2	43^2	337^2	(c)	

Table 2.3: non-trivial ($\mathcal{O}_{K_t} \supsetneq \mathbb{Z}[\theta_t]$, $\mathfrak{C}_{K_t}$: principal) cases

Chapter 3

Relative cyclic extensions of prime degree

In this chapter, we provide a generalization of the results obtained in Chapter 2 and an application. The outline is as follows. It is known that any cyclic cubic field is generated by a root of Shanks cubic polynomial with a parameter $t \in \mathbb{Q}$. First, we introduce Rikuna's generic cyclic polynomial [16], a polynomial that can be regarded as a generalization of Shanks cubic polynomial. Next, we give a sufficient condition for the monogenity of a cyclic extension over $\mathbb{Q}(\zeta + \zeta^{-1})$ of odd prime degree l and the examples, where ζ is a primitive l-th root of unity. The main tool used in the proof is Newton polygon (as in Chapter 2). Finally, we prove that there exist infinitely many monogenic cyclic extensions over $\mathbb{Q}(\zeta + \zeta^{-1})$ of degree $l \geq 5$. The condition can be written using certain ideals. It is difficult to count ideals in general because of the possibility of duplication. However we can attribute the counting of ideals to the counting of elements by using Shintani's fundamental domain. We obtain the result by the evaluation of an infinite series which is an analogue of Dedekind's zeta function whose ideal runs through the prime ideals.

3.1 Rikuna's generic cyclic polynomial

Let $n \geq 3$ be an integer and k be a field whose characteristic does not divide n. Assume that k contains $\omega := \zeta + \zeta^{-1}$ where ζ is a primitive n-th root of unity. Then we define $p(X), q(X) \in k[X]$ and $F_u(X) \in k(u)[X]$ by

$$\begin{aligned} p(X) &= \frac{\zeta^{-1}(X-\zeta)^n - \zeta(X-\zeta^{-1})^n}{\zeta^{-1}-\zeta}, \\ q(X) &= \frac{(X-\zeta)^n - (X-\zeta^{-1})^n}{\zeta^{-1}-\zeta}, \\ F_u(X) &= p(X) - uq(X) \end{aligned}$$

where u is a variable. $F_u(X)$ is called *Rikuna's generic cyclic polynomial.* For further details, see [16]. Assume that n is an odd prime number l. Then we define

$$\Omega_s(X) = p(X) - \frac{s}{l} q(X)$$

where s is a variable. We introduce $\Omega_s(X)$ for $l = 3, 5$.

- If $l = 3$,
$$\Omega_s(X) = X^3 - sX^2 - (s+3)X - 1.$$
This corresponds with Shanks cubic polynomial.

- If $l = 5$,
$$\Omega_s(X) = X^5 - sX^4 + 2(\omega s - 5)X^3 + 2\omega(s+5)X^2 - (s - 5\omega)X - 1.$$

We can consider that $\Omega_s(X)$ is a generalization of Shanks cubic polynomial. For further details, see [12].

In the following we assume that k is a number field containing ω and that $s \in \mathcal{O}_k$. Then $\Omega_s(X) \in \mathcal{O}_k[X]$. Let θ_s be a root of $\Omega_s(X)$. Put $K_s := k(\theta_s)$. We introduce the following facts.

- K_s/k is a cyclic extension of degree l. We put
$$G := \mathrm{Gal}(K_s/k) = \langle \sigma \rangle = \{e, \sigma, \dots, \sigma^{l-1}\}.$$

- θ_s is a unit in K_s satisfying that (if necessary by replacing σ)
$$N(\theta_s) = 1, \quad Tr(\theta_s) = s, \quad \sigma^j(\theta_s) = \frac{\nu_{j+1}\theta_s - \nu_j}{\nu_j\theta_s - \nu_{j-1}} \quad \text{where} \quad \nu_j := \frac{\zeta^j - \zeta^{-j}}{\zeta - \zeta^{-1}} \tag{3.1}$$
for $j \in \{0, 1, \dots, l-1\}$. We abbreviate as $N := N_{K_s/k}$ and $Tr := Tr_{K_s/k}$. We clearly have $\nu_j \in k$ and
$$\nu_j = \omega\nu_{j-1} - \nu_{j-2} \ (j \geq 2). \tag{3.2}$$

- Let Δ_s be a principal ideal of k generated by $s^2 - l\omega s + l^2$. Δ_s^{l-1} is equal to an ideal generated by the discriminant of $\Omega_s(X)$ [12, Proposition 5.3]. Namely, it holds that
$$\Delta_s^{l-1} = \left(N\left(\prod_{\sigma \neq e} (\theta_s - \sigma(\theta_s)) \right) \right).$$

- Let $\mathfrak{c}_{K_s/k}$ and $\mathfrak{d}_{K_s/k}$ be the conductor and the discriminant, respectively. We obtain
$$\mathfrak{c}_{K_s/k}^{l-1} = \mathfrak{d}_{K_s/k} \mid \Delta_s^{l-1}.$$
The relation $\mathfrak{c}_{K_s/k}^{l-1} = \mathfrak{d}_{K_s/k}$ follows from the conductor-discriminant formula.

3.2 A sufficient condition for the monogenity

In this section we provide a sufficient condition for the monogenity of relative cyclic extensions of prime degree (Theorem 3.2.1). Let k be a number field and $\mathfrak{p}$ be a prime ideal of k. We denote by P_k the group of all principal ideals, and by $v_{\mathfrak{p}}(\mathfrak{a})$ the $\mathfrak{p}$-adic valuation of an ideal $\mathfrak{a}$ of k defined by

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

where $\mathfrak{p}$ runs through the prime ideals in k.

Theorem 3.2.1. *Let l be an odd prime number and $k = \mathbb{Q}(\omega)$ with $\omega = \zeta + \zeta^{-1}$ where ζ is a primitive l-th root of unity. Let $s \in \mathcal{O}_k$, and K_s, Δ_s, $\mathfrak{c}_{K_s/k}$ be as in Section 3.1. If $\Delta_s \mathfrak{c}_{K_s/k}^{-1} \in P_k^l := \{\mathfrak{a}^l \mid \mathfrak{a} \in P_k\}$, then K_s/k has a power integral basis. Moreover, we write $\Delta_s \mathfrak{c}_{K_s/k}^{-1} = (b)^l$ with $b \in \mathcal{O}_k$. Then we have*

$$\mathcal{O}_{K_s} = \mathcal{O}_k \left[\frac{\theta_s - a}{b}\right]$$

with $a \in \mathcal{O}_k$ satisfying $a \equiv sl^{-1} \bmod (b)$.

Proof. It suffices to show that

$$\frac{\theta_s - a}{b} \in \mathcal{O}_{K_s}$$

for $a \in \mathcal{O}_k$ since we clearly have

$$d_{K_s/k}\left(\frac{\theta_s - a}{b}\right) = \frac{d_{K_s/k}(\theta_s)}{b^{l(l-1)}} = \mathfrak{c}_{K_s/k}^{l-1} = \mathfrak{d}_{K_s/k}.$$

An ideal $(\sigma(\theta_s) - \theta_s)$ is ambiguous, namely $\sigma\left(\sigma(\theta_s) - \theta_s\right) = (\sigma(\theta_s) - \theta_s)$, because it holds

$$\frac{\sigma\left(\sigma(\theta_s) - \theta_s\right)}{\sigma(\theta_s) - \theta_s} = \frac{\frac{(\omega^2-1)\theta_s - \omega}{\omega\theta_s - 1} - \frac{\omega\theta_s - 1}{\theta_s}}{\frac{\omega\theta_s - 1}{\theta_s} - \theta_s} = \frac{1}{\omega\theta_s - 1} = \frac{1}{\theta_s \sigma\left(\theta_s\right)} \in \mathcal{O}_{K_s}^{\times}$$

from (3.1) where $\mathcal{O}_{K_s}^{\times}$ is the unit group of K_s. Hence we obtain $N\left(\theta_s - \sigma(\theta_s)\right) = \left(\theta_s - \sigma(\theta_s)\right)^l$. On the other hand, it holds that $N\left(\theta_s - \sigma(\theta_s)\right) = \Delta_s = \mathfrak{c}_{K_s/k}(b)^l$. Hence we have

$$\theta_s \equiv \sigma(\theta_s) \bmod (b). \tag{3.3}$$

Let $\mathfrak{p}_l$ be the unique prime ideal over l in k, namely $\mathfrak{p}_l = (\omega - 2)$. We divide the situation into two cases;

(i) Assume $\mathfrak{p}_l \nmid (b)$. Then there exists $a \in \mathcal{O}_k$ satisfying $a \equiv sl^{-1} \bmod (b)$ by $l \in (\mathcal{O}_k / b\mathcal{O}_k)^{\times}$. From (3.3) we obtain

$$a \equiv sl^{-1} = Tr(\theta_s) l^{-1} \equiv l\theta_s l^{-1} = \theta_s \bmod (b).$$

Hence we have $\frac{\theta_s - a}{b} \in \mathcal{O}_{K_s}$.

(ii) Assume $\mathfrak{p}_l \mid (b)$. Put $a = \frac{s}{l}$. Then we have $a \in \mathcal{O}_k$ and $v_{\mathfrak{p}_l}(b) = 1$ by Lemma 3.3.4. Thus it holds that

$$a = \frac{s}{l} = \frac{Tr(\theta_s)}{l} \equiv \theta \bmod \left(\frac{b}{\omega - 2}\right)$$

from (3.3), that is $\theta_s - a \in \frac{b}{\omega-2}\mathcal{O}_{K_s}$. On the other hand, $v_{\mathfrak{p}_l}(\theta_s - a) \geq 1$ by considering the Newton polygon because the $\mathfrak{p}_l$-adic valuations of all of the coefficients of the minimal polynomial are greater than 1 by Proposition 3.3.5 and (3.5). Hence we have $\frac{\theta_s - a}{b} \in \mathcal{O}_{K_s}$.

Then the assertion is clear. □

In the next section we prove Lemma 3.3.4 and Proposition 3.3.5 which we used in the above proof.

Remark 3.2.2. *If $l = 3$, then the condition $\Delta_s \mathfrak{c}_{K_s/k}^{-1} \in P_k^l$ in* Theorem 3.2.1 *is the necessary and sufficient condition* (Theorem 2.5.1).

We say that an integral ideal is square-free if it is not divided by the square of a prime ideal. From Theorem 3.2.1 we have the following.

Corollary 3.2.3. *If Δ_s is square-free, then $\mathcal{O}_{K_s} = \mathcal{O}_k[\theta_s]$.*

Proof. The ideal Δ_s consists of the prime ideals of k ramified in K_s because the ideal $(\sigma(\theta_s) - \theta_s)$ is ambiguous and $\Delta_s = N(\theta_s - \sigma(\theta_s))$ is square-free. By $\mathfrak{c}_{K_s/k} \mid \Delta_s$, we have $\mathfrak{c}_{K_s/k} = \Delta_s$. Namely, $\mathfrak{d}_{K_s/k} = d_{K_s/k}(\theta_s)$. □

Remark 3.2.4. *As an application of* Corollary 3.2.3*, we prove that there exist infinitely many monogenic cyclic extensions of odd prime degree $l(\geq 5)$ over a suitable base field* (Theorem 3.5.1).

3.3 Minimal polynomial of $\theta_s - \frac{s}{l}$

The purpose of this section is to prove Lemma 3.3.4 and Proposition 3.3.5. This completes the proof of Theorem 3.2.1.

Let l be an odd prime number and $k = \mathbb{Q}(\omega)$. Let $s \in \mathcal{O}_k$, and K_s, Δ_s, $\mathfrak{c}_{K_s/k}$ be as in Section 3.1. We prepare the following lemma.

Lemma 3.3.1. *Let $m \leq l$ be a positive integer and $n_1, \ldots, n_m \in \{0, 1, \ldots, l-1\}$ be any integers different from each other. Then the value of $Tr\left(\sigma^{n_1}(\theta_s) \cdots \sigma^{n_m}(\theta_s)\right)$ depends only on m.*

Remark 3.3.2. *For example, it holds that $Tr(\theta_s \theta_s^{\sigma}) = Tr(\theta_s \theta_s^{\sigma^2})$. This equation is trivial when $l = 3$, but nontrivial when $l \geq 5$. If θ_s is replaced by an arbitrary element of K_s, this does not work generally.*

Proof. It is obvious when $m = 1$. Assume $m = 2$. Let i, j be integers and $1 \leq j \leq l - 1$. From (3.1) and (3.2) it holds that

$$\nu_j \sigma^i(\theta_s)\sigma^{j+i}(\theta_s) - \nu_{j-1}\sigma^{j+i}(\theta_s) = \omega\nu_j\sigma^i(\theta_s) - \nu_{j-1}\sigma^i(\theta_s) - \nu_j. \tag{3.4}$$

Hence we have

$$Tr\left(\sigma^i(\theta_s)\sigma^{j+i}(\theta_s)\right) = \omega\, Tr(\theta_s) - Tr(1) = \omega s - l.$$

We can replace i and j to satisfy $n_1 = i$ and $n_2 = j + i$. Namely, the assertion is proved for $m = 2$. Assume $m = 3$. Then we can prove the assertion in the same way by multiplying (3.4) by $\sigma^{n_3}(\theta_s)$. By repeating inductively this argument, the assertion is proved. □

We denote the minimal polynomial of $\theta_s - \frac{s}{l}$ as

$$X^l + a_1X^{l-1} + a_2X^{l-2} + a_3X^{l-3} + \cdots + a_{l-1}X + a_l$$

with $a_i \in k$. Put $\Theta := \theta_s - \frac{s}{l}$ and $T_j := Tr\left(\sigma^{n_1}(\Theta)\sigma^{n_2}(\Theta)\cdots\sigma^{n_j}(\Theta)\right)$ where $n_1, n_2, \cdots, n_j \in \{0, 1, \ldots, l-1\}$ are different from each other. Note that the value of T_j is independent of choosing $n_1, n_2, \cdots, n_j$ from Lemma 3.3.1. Hence we have

$$a_j = (-1)^j \frac{(l-1)!}{j!(l-j)!} T_j. \tag{3.5}$$

We prove Proposition 3.3.5 with the following lemmas.

Lemma 3.3.3. *Let j be an integer satisfying $3 \leq j \leq l$. Then it holds that*

$$T_j = -\frac{2s - l\omega}{l} T_{j-1} - \frac{s^2 - l\omega s + l^2}{l^2} T_{j-2}. \tag{3.6}$$

Proof. Put $a = \frac{s}{l}$. From (3.1) it holds that

$$\sigma^j(\Theta) + a = \sigma^j(\theta_s) - a + a = \frac{\nu_{j+1}\theta_s - \nu_{j+1}a + \nu_{j+1}a - \nu_j}{\nu_j\theta_s - \nu_j a + \nu_j a - \nu_{j-1}} = \frac{\nu_{j+1}\Theta + \nu_{j+1}a - \nu_j}{\nu_j\Theta + \nu_j a - \nu_{j-1}}.$$

In the same way as the proof of Lemma 3.3.1 we obtain

$$T_2 = -\frac{2s - l\omega}{l} T_1 - \frac{s^2 - l\omega s + l^2}{l^2} Tr(1).$$

By repeating inductively this argument, we have (3.6). The assertion is clear. □

Lemma 3.3.4. *Let $\mathfrak{p}_l$ be the unique prime ideal over l in k. Then it holds that*

$$v_{\mathfrak{p}_l}\left(s^2 - l\omega s + l^2\right) \in \{0, 2, 4, \ldots, l-3, l-1, l\}.$$

Proof. We clearly have

$$v_{\mathfrak{p}_l}\left(s^2 - l\omega s + l^2\right) = \begin{cases} 0 & \left(v_{\mathfrak{p}_l}(s) = 0\right), \\ 2v_{\mathfrak{p}_l}(s) & \left(1 \leq v_{\mathfrak{p}_l}(s) < \frac{l-1}{2}\right), \\ l - 1 + v_{\mathfrak{p}_l}(s'^2 - \omega s' + 1) & \left(v_{\mathfrak{p}_l}(s) = \frac{l-1}{2}\right), \\ l - 1 & \left(v_{\mathfrak{p}_l}(s) < \frac{l-1}{2}\right) \end{cases}$$

where $s' = \frac{s}{l} \in \mathcal{O}_k$. Assume that $v_{\mathfrak{p}_l}(s) = \frac{l-1}{2}$ and $v_{\mathfrak{p}_l}(s'^2 - \omega s' + 1) \geq 1$. Then we can write $s' = 1 + (\omega - 2)s''$ with $s'' \in \mathcal{O}_k$ because it holds that

$$s'^2 - \omega s' + 1 \equiv s'^2 - 2s' + 1 = (s' - 1)^2 \bmod \mathfrak{p}_l.$$

Thus we obtain

$$s'^2 - \omega s' + 1 = (1 + (\omega - 2)s'')^2 - \omega(1 + (\omega - 2)s'') + 1 = (\omega - 2)\left\{(\omega - 2)(s'' - 1)s'' - 1\right\}.$$

Hence we have $v_{\mathfrak{p}_l}(s'^2 - \omega s' + 1) = 1$. The assertion is clear. □

Proposition 3.3.5. *Let $\mathfrak{p}_l$ be the unique prime ideal over l in k. Assume that $\Delta_s \mathfrak{c}_{K_s/k}^{-1} \in P_k^l$ and $\mathfrak{p}_l \mid \Delta_s \mathfrak{c}_{K_s/k}^{-1}$. Namely, we may write $(b)^l = \Delta_s \mathfrak{c}_{K_s/k}^{-1}$ with $b \in \mathcal{O}_k$. Then, for any positive even integer $i \leq l - 1$ we have*

$$\begin{aligned} v_{\mathfrak{p}_l}\left(T_i\right) &= \frac{i}{2} v_{\mathfrak{p}_l}\left(\Delta_s\right) - (i - 1)v_{\mathfrak{p}_l}(l) = \frac{l + i - 1}{2}, \\ v_{\mathfrak{p}_l}\left(T_{i+1}\right) &= \frac{i}{2} v_{\mathfrak{p}_l}\left(\Delta_s\right) + v_{\mathfrak{p}_l}\left(\Delta'_s\right) - i v_{\mathfrak{p}_l}(l) \geq \frac{l + i + 1}{2} \end{aligned} \tag{3.7}$$

where Δ'_s is a principal ideal of k generated by $2s - l\omega \in \mathcal{O}_k$.

Proof. By abuse of notation we denote $s^2 - l\omega s + l^2$, $2s - l\omega \in \mathcal{O}_k$ by Δ_s, Δ'_s, respectively. We have $v_{\mathfrak{p}_l}(\Delta_s) = l$ and $v_{\mathfrak{p}_l}\left(\Delta'_s\right) \geq \frac{l+1}{2}$ from the assumption, Lemma 3.3.4 and $(\Delta'_s)^2 = 4\Delta_s + l^2(\omega^2 - 4)$. Assume $i = 2$. Then we clearly have

$$T_2 = Tr\left(\theta_s \sigma(\theta_s)\right) - \frac{2s}{l} Tr(\theta_s) + \frac{s^2}{l} = -\frac{\Delta_s}{l}, \qquad T_3 = -\frac{\Delta'_s}{l} T'_2 = \frac{\Delta_s \Delta'_s}{l^2}.$$

from the definition of T_2 and (3.6). Hence we obtain

$$v_{\mathfrak{p}_l}(T_2) = v_{\mathfrak{p}_l}(\Delta_s) - v_{\mathfrak{p}_l}(l) = \frac{l + 1}{2}, \qquad v_{\mathfrak{p}_l}(T_3) = v_{\mathfrak{p}_l}(\Delta_s \Delta'_s) - v_{\mathfrak{p}_l}(l^2) \geq \frac{l + 3}{2}.$$

Assume that it holds that (3.7) for a positive even integer $i - 2 \leq l - 3$. Then we obtain

$$\begin{aligned} v_{\mathfrak{p}_l}(T_i) &= \min\left\{ v_{\mathfrak{p}_l}\left(\frac{\Delta'_s}{l} T_{i-1}\right), v_{\mathfrak{p}_l}\left(\frac{\Delta_s}{l^2} T_{i-2}\right)\right\} = v_{\mathfrak{p}_l}\left(\frac{\Delta_s}{l^2} T_{i-2}\right) = \frac{l + i - 1}{2}, \\ v_{\mathfrak{p}_l}(T_{i+1}) &= \min\left\{ v_{\mathfrak{p}_l}\left(\frac{\Delta'_s}{l} T_i\right), v_{\mathfrak{p}_l}\left(\frac{\Delta_s}{l^2} T_{i-1}\right)\right\} \geq \frac{l + i + 1}{2} \end{aligned}$$

from $v_{\mathfrak{p}_l}\left(\frac{\Delta'_s}{l}\right) \geq 1$, $v_{\mathfrak{p}_l}\left(\frac{\Delta_s}{l^2}\right) = 1$, and (3.6). □

3.4 Examples

We introduce the examples for $l = 5$. Table 3.1 below is a list of s, the prime factorization of $\mathfrak{c}_{K_s}$, the prime factorization of Δ_s, where $\mathfrak{p}_p$ is a prime ideal over p of k and $\mathfrak{p}'_p$ is a conjugate of $\mathfrak{p}_p$ splitting in $k/\mathbb{Q}$. There are 3 “cases”:

(a) K_s/k has a power integral basis with a (trivial) generator θ_s by Theorem 3.2.1, namely $\Delta_s = \mathfrak{c}_{K_s/k}$.

(b) K_s/k has a power integral basis by Theorem 3.2.1 but is a non-trivial case, namely $\frac{\Delta_s}{\mathfrak{c}_{K_s/k}} \in P_k^l \setminus \{e\}$.

(c) We can not determine whether K_s/k has a power integral basis or not by Theorem 3.2.1.

s	$\mathfrak{c}_{K_s/k}$	Δ_s	case
0	$\mathfrak{p}_5^3$	$\mathfrak{p}_5^4$	(c)
1	$\mathfrak{p}_{11} \quad \mathfrak{p}_{71}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{71}$	(a)
2	$\mathfrak{p}_{1031}$	$\mathfrak{p}_{1031}$	(a)
3	$\mathfrak{p}_{11} \quad \mathfrak{p}_{131}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{131}$	(a)
4	$\mathfrak{p}_{11} \quad \mathfrak{p}_{191}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{191}$	(a)
5	$\mathfrak{p}_5^3$	$\mathfrak{p}_5^5$	(c)
ω	$\mathfrak{p}_{11} \quad \mathfrak{p}_{31}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{31}$	(a)
$1+\omega$	$\mathfrak{p}_{461}$	$\mathfrak{p}_{461}$	(a)
$2+\omega$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{61}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{61}$	(a)
$3+\omega$	$\mathfrak{p}_5^2 \quad \mathfrak{p}_{41}$	$\mathfrak{p}_5^2 \quad \mathfrak{p}_{41}$	(a)
$4+\omega$	$\mathfrak{p}_{1601}$	$\mathfrak{p}_{1601}$	(a)
$5+\omega$	$\mathfrak{p}_{41} \quad \mathfrak{p}_{61}$	$\mathfrak{p}_{41} \quad \mathfrak{p}_{61}$	(a)
2ω	$\mathfrak{p}_{211}$	$\mathfrak{p}_{211}$	(a)
$1+2\omega$	$\mathfrak{p}_5^2 \quad \mathfrak{p}_{11}$	$\mathfrak{p}_5^2 \quad \mathfrak{p}_{11}$	(a)
$2+2\omega$	$\mathfrak{p}_{421}$	$\mathfrak{p}_{421}$	(a)
$3+2\omega$	$\mathfrak{p}_{691}$	$\mathfrak{p}_{691}$	(a)
$4+2\omega$	$\mathfrak{p}_{1151}$	$\mathfrak{p}_{1151}$	(a)
$5+2\omega$	$\mathfrak{p}_{31} \quad \mathfrak{p}_{61}$	$\mathfrak{p}_{31} \quad \mathfrak{p}_{61}$	(a)
3ω	$\mathfrak{p}_{211}$	$\mathfrak{p}_{211}$	(a)
$1+3\omega$	$\mathfrak{p}_{211}$	$\mathfrak{p}_{211}$	(a)
$2+3\omega$	$\mathfrak{p}_{281}$	$\mathfrak{p}_{281}$	(a)
$3+3\omega$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{41}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{41}$	(a)
$4+3\omega$	$\mathfrak{p}_5^2 \quad \mathfrak{p}_{31}$	$\mathfrak{p}_5^2 \quad \mathfrak{p}_{31}$	(a)
$5+3\omega$	$\mathfrak{p}_{11} \quad \mathfrak{p}'_{11}$	$\mathfrak{p}_{11} \quad {\mathfrak{p}'_{11}}^2$	(c)
4ω	$\mathfrak{p}_{11} \quad \mathfrak{p}_{31}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{31}$	(a)
$1+4\omega$	$\mathfrak{p}_{281}$	$\mathfrak{p}_{281}$	(a)
$2+4\omega$	$\mathfrak{p}_5^2 \quad \mathfrak{p}_{11}$	$\mathfrak{p}_5^2 \quad \mathfrak{p}_{11}$	(a)
$3+4\omega$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{31}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{31}$	(a)
$4+4\omega$	$\mathfrak{p}_{521}$	$\mathfrak{p}_{521}$	(a)
$5+4\omega$	$\mathfrak{p}_{881}$	$\mathfrak{p}_{881}$	(a)
5ω	$\mathfrak{p}_5^3$	$\mathfrak{p}_5^4$	(c)
$1+5\omega$	$\mathfrak{p}_{521}$	$\mathfrak{p}_{521}$	(a)
$2+5\omega$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{41}$	$\mathfrak{p}_{11} \quad \mathfrak{p}_{41}$	(a)
$3+5\omega$	$\mathfrak{p}_{421}$	$\mathfrak{p}_{421}$	(a)
$4+5\omega$	$\mathfrak{p}_{461}$	$\mathfrak{p}_{461}$	(a)
$5+5\omega$	$\mathfrak{p}_5^3$	$\mathfrak{p}_5^4$	(c)
$50+40\omega$	$\mathfrak{p}_{211}$	$\mathfrak{p}_5^5 \quad \mathfrak{p}_{211}$	(b)

Table 3.1: Examples for $l = 5$

For example,

- K_1, K_2, K_3, K_4 have power integral bases over k since $s = 1, 2, 3, 4$ satisfy $\Delta_s = \mathfrak{c}_{K_s/k}$.
- $K_{50+40\omega}/k$ has a power integral basis and $\mathcal{O}_{K_{50+40\omega}} = \mathcal{O}_k\left[\frac{\theta_s-8s-10}{\omega-2}\right]$ by Theorem 3.2.1.
- K_0 can not determine whether K_s/k has a power integral basis or not by Theorem 3.2.1.

Remark 3.4.1. *Note that the cases are different from the cases for $l = 3$* (Section 2.6)*. There may exist more than one parameter s' satisfying $K_s = K_{s'}$ for a parameter s. However such a parameter has not been completely determined for $l \geq 5$ yet. This is one of the problems to obtaining equivalence conditions of the monogenity for K_s/k of odd prime degree $l \geq 5$.*

3.5 An application: infinite families of monogenic extensions

In this section we prove the following theorem.

Theorem 3.5.1. *Let $l \geq 5$ be an odd prime number and $k = \mathbb{Q}(\omega)$ with $\omega = \zeta + \zeta^{-1}$ where ζ is a primitive l-th root of unity. Let $s \in \mathcal{O}_k$, and K_s, θ_s be as in Section 3.1. Then there exist infinitely many cyclic extensions K_s/k satisfying $\mathcal{O}_{K_s} = \mathcal{O}_k[\theta_s]$.*

Remark 3.5.2. *For an odd prime number $l \geq 5$, the number of monogenic extensions of degree l over $\mathbb{Q}$ is one or zero* [6]*. However,* Theorem 3.5.1 *indicates that the number of those over $\mathbb{Q}(\omega)$ is infinite.*

Remark 3.5.3. *D. S. Dummit and H. Kisilevsky proved that there exist infinitely many monogenic and non-monogenic cyclic cubic fields, namely the case of $l = 3$. Our proof of* Theorem 3.5.1 *is based on their proof of* [4, Theorem 3].

Proof. Put $\epsilon = \omega + 2$. ϵ is a totally positive unit of k. Put

$$R = \mathbb{Z}_{\geq 0} + \mathbb{Z}_{\geq l}\epsilon + \mathbb{Z}_{\geq 0}\epsilon^2 + \cdots + \mathbb{Z}_{\geq 0}\epsilon^{\frac{l-3}{2}} \subset \mathcal{O}_k$$

where $\mathbb{Z}_{\geq 0}$ (resp. $\mathbb{Z}_{\geq l}$) is the set of integers greater than or equal to 0 (resp. l). It suffices to show that there exist infinitely many $s \in R$ such that Δ_s is square-free. Actually, assume that Δ_s is square-free, then $\mathcal{O}_{K_s} = \mathcal{O}_k[\theta_s]$ from Corollary 3.2.3. If the different ideals $\Delta_s, \Delta_{s'} (s, s' \in R)$ are square-free, then we have $K_s \neq K_{s'}$ from $\mathfrak{d}_{K_s/k} = \Delta_s^{l-1} \neq \Delta_{s'}^{l-1} = \mathfrak{d}_{K_{s'}/k}$. On the other hand, put $s = a_0 + a_1\epsilon + \cdots + a_{\frac{l-3}{2}}\epsilon^{\frac{l-3}{2}} \in R$, then we have

$$\begin{aligned} s^2 - l\omega s + l^2 &= \left(a_0 + a_2\epsilon^2 + a_3\epsilon^3 + \cdots + a_{\frac{l-3}{2}}\epsilon^{\frac{l-3}{2}}\right)s + (a_1 - l)\epsilon s + 2ls + l^2 \\ &\in \mathbb{Z}_{\geq 0} + \mathbb{Z}_{\geq 0}\epsilon + \cdots + \mathbb{Z}_{\geq 0}\epsilon^{l-3}. \end{aligned}$$

The map

$$R \to \mathbb{Z}_{\geq 0} + \mathbb{Z}_{\geq 0}\epsilon + \cdots + \mathbb{Z}_{\geq 0}\epsilon^{l-3}, \ s \mapsto s^2 - l\omega s + l^2$$

is injective because $s^2 - l\omega s + l^2 = (s - \frac{l\omega}{2})^2 - \frac{l^2\omega^2}{4} + l^2$ and $R \subset [\frac{l\omega}{2}, \infty)$. Now we introduce a Shintani's fundamental domain D of $(k \otimes \mathbb{R})_+/\mathcal{O}_{k,+}^\times$. Here $(k \otimes \mathbb{R})_+$ denotes the totally positive part of $k \otimes_{\mathbb{Q}} \mathbb{R}$. Then there exists a natural action of the group $\mathcal{O}_{k,+}^\times$ of totally positive units of k. Shintani showed that we can take a fundamental domain D of $(k \otimes \mathbb{R})_+/\mathcal{O}_{k,+}^\times$ as a finite disjoint union of open simplicial cones [21]. That is we can write

$$(k \otimes \mathbb{R})_+ = \coprod_{u \in \mathcal{O}_{k,+}^\times} uD.$$

Considering $\{s^2 - l\omega s + l^2 \mid s \in R\} \subset (k \otimes \mathbb{R})_+$, we can take a finite number of $u_i \in \mathcal{O}_{k,+}^\times$ so that

$$\{s^2 - l\omega s + l^2 \mid s \in R\} \subset \coprod_i u_i D.$$

Let L be the number of such u_i's. Then we have for any fixed $s \in R$

$$\sharp \{\Delta_t \mid t \in R, \Delta_t = \Delta_s\} \leq L$$

where $\sharp$ denotes the number of elements in a set. Hence, it suffices to show that there exist infinitely many $s \in R$ such that Δ_s is square-free. Let n be a positive integer. We define R_n, N_n and M_n by

$$\begin{aligned} R_n &= \left\{ \sum_{i=0}^{\frac{l-3}{2}} a_i \epsilon^i \in R \mid a_1 < n + l,\ a_i < n (i \neq 1) \right\}, \\ N_n &= \{s \in R_n \mid \Delta_s \text{ is square-free}\}, \\ M_n &= \{s \in R_n \mid \Delta_s \text{ is not square-free}\}. \end{aligned}$$

Then we easily have

$$\sharp N_n = \sharp R_n - \sharp M_n = n^{\frac{l-1}{2}} - \sharp M_n. \tag{3.8}$$

Let $\mathfrak{p}$ be a prime ideal of k and p be a prime number under $\mathfrak{p}$. Then we easily have

$$\sharp M_n \leq \sum_{\mathfrak{p}} \sharp \left\{ s \in R_n \mid s^2 - l\omega s + l^2 \equiv 0 \bmod \mathfrak{p}^2 \right\} \tag{3.9}$$

where $\mathfrak{p}$ runs through the prime ideals of k. We divide the situation into two cases;

(i) Assume that $\mathfrak{p} \nmid (l)$, namely $p \neq l$. Let f_p be the degree of the field extension $[\mathcal{O}_k/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$. We define $R_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ by

$$\begin{aligned} R_{\mathfrak{p}} &= \left\{ \sum_{i=0}^{f_p - 1} a_i \epsilon^i \in R \mid a_1 < p^2 + l,\ a_i < p^2 (i \neq 1) \right\}, \\ B_{\mathfrak{p}} &= \coprod_{a_i' = 0}^{[\frac{n}{p^2}]+1} \left(R_{\mathfrak{p}} + \sum_{i=0}^{f_p - 1} a_i' p^2 \epsilon^i \right) \end{aligned}$$

where [ ] denotes the Gauss sign. Then we have

$$R_n \subset \coprod_{a''_j=0}^{n-1} \left(B_{\mathfrak{p}} + \sum_{j=f_p}^{\frac{l-3}{2}} a''_j \epsilon^j \right). \tag{3.10}$$

On the other hand, a natural map $R_{\mathfrak{p}} \to \mathcal{O}_k/\mathfrak{p}^2$ is written by

$$s = \sum_{i=0}^{f_p-1} a_i \epsilon^i \mapsto \sum_{i=0}^{f_p-1} b_i \epsilon^i + p \sum_{i=0}^{f_p-1} c_i \epsilon^i$$

with $b_i, c_i \in \{0, 1, \ldots, p-1\}$ satisfying $a_i \equiv b_i + pc_i \bmod p^2$. This map is bijective because of the uniqueness of a $\mathfrak{p}$-adic expansion and $\mathcal{O}_k/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}(\epsilon)$. Let $t \in R$. In the same way, a natural map $R_{\mathfrak{p}} + t := \{s + t \mid s \in R_{\mathfrak{p}}\} \to \mathcal{O}_k/\mathfrak{p}^2$ is bijective. Hence we have

$$\sharp \left\{ s \in R_n \mid s^2 - l\omega s + l^2 \equiv 0 \bmod \mathfrak{p}^2 \right\} \leq \sum_{a''_j} \sum_{a'_i} 2 = 2n^{\frac{l-1}{2} - f_p} \left(\left[\frac{n}{p^2} \right] + 2 \right)^{f_p} \tag{3.11}$$

from (3.10) and Lemma 3.5.4.

(ii) Assume that $\mathfrak{p} \mid (l)$, namely $p = l$ and $\mathfrak{p} = (\omega - 2)$. Put

$$R_{\mathfrak{p}} = \{a_0 + a_1 \epsilon \in R \mid a_0 < l, a_1 < 2l\}.$$

A natural map $R_{\mathfrak{p}} \to \mathcal{O}_k/\mathfrak{p}^2$ is bijective because of a uniqueness of a $\mathfrak{p}$-adic expansion and $\mathcal{O}_k/\mathfrak{p} \simeq \mathbb{Z}/l\mathbb{Z}$, $\epsilon = \omega + 2$. As with (i), we have

$$\sharp \left\{ s \in R_n \mid s^2 - l\omega s + l^2 \equiv 0 \bmod \mathfrak{p}^2 \right\} \leq l n^{\frac{l-1}{2} - 2} \left(\left[\frac{n}{l} \right] + 2 \right)^2. \tag{3.12}$$

From (3.9) and (3.11), (3.12), we have

$$\begin{aligned} \sharp M_n &\leq \sum_{\mathfrak{p} \nmid (l)} 2n^{\frac{l-1}{2} - f_p} \left(\left[\frac{n}{p^2} \right] + 2 \right)^{f_p} + l n^{\frac{l-1}{2} - 2} \left(\left[\frac{n}{l} \right] + 2 \right)^2 \\ &\leq \left(\sum_{\mathfrak{p} \nmid (l)} \frac{2}{p^{2f_p}} + \frac{1}{l} \right) n^{\frac{l-1}{2}} + o(n^{\frac{l-1}{2}}) \end{aligned}$$

where o denotes Landau's symbol. From (3.8), we have

$$\sharp N_n \geq \left(1 - \frac{1}{l} - \sum_{\mathfrak{p} \nmid (l)} \frac{2}{p^{2f_p}} \right) n^{\frac{l-1}{2}} + o(n^{\frac{l-1}{2}}).$$

In the following, we prove $1-\frac{1}{l}-\sum_{\mathfrak{p}\nmid(l)}\frac{2}{p^{2f_p}}>0$. From Lemma 3.5.5, we have

$$1-\frac{1}{l}-\sum_{\mathfrak{p}\nmid(l)}\frac{2}{p^{2f_p}}=\frac{l-1}{l}-2\sum_{\mathfrak{p}\nmid(l)}\frac{1}{N(\mathfrak{p})^2}\geq\frac{l-1}{l}-\frac{4l^2}{(l+1)^2(l-1)}=\frac{l^4-4l^3-2l^2+1}{l(l+1)^2(l-1)}$$

where N denotes the absolute norm of k. Since $l^4-4l^3-2l^2+1>0$, it holds that $1-\frac{1}{l}-\sum_{\mathfrak{p}\nmid(l)}\frac{2}{p^{2f_p}}>0$. Hence, we have $\sharp N_n\to\infty$ as $n\to\infty$. The assertion is clear. □

In the following, we prove Lemma 3.5.4 and Lemma 3.5.5 which we used in the above proof.

Lemma 3.5.4. *Let $l\geq 5$ be an odd prime number and $k=\mathbb{Q}(\omega)$. Let $\mathfrak{p}$ be a prime ideal of k. The congruence $s^2-l\omega s+l^2\equiv 0 \bmod \mathfrak{p}^2$ has at most two solutions on $\mathcal{O}_k/\mathfrak{p}^2$ except for $\mathfrak{p}=(\omega-2)$. On the other hand, if $\mathfrak{p}=(\omega-2)$, then this congruence has l solutions.*

Proof. Let $\mathfrak{p}\neq(\omega-2)$. The congruence $s^2-l\omega s+l^2\equiv 0 \bmod \mathfrak{p}$ has at most two solutions on the field $\mathcal{O}_k/\mathfrak{p}$. Let s_0 be the solution of the congruence and $\pi\in\mathfrak{p}\backslash\mathfrak{p}^2$. Put $a_1=s_0+t_1\pi$ and $a_2=s_0+t_2\pi$ with the different elements $t_1,t_2\in\mathcal{O}_k/\mathfrak{p}$. Assume that $a_i(i=1,2)$ satisfy $a_i^2-l\omega a_i+l^2\equiv 0 \bmod \mathfrak{p}^2$. Then we have

$$(a_1-a_2)(a_1+a_2-l\omega)\equiv 0 \bmod \mathfrak{p}^2.$$

Since $a_1-a_2=(t_1-t_2)\pi$ and $a_1+a_2-l\omega=2s_0+(t_1+t_2)\pi-l\omega$, it holds that $2s_0-l\omega\equiv 0 \bmod \mathfrak{p}$. Then we have

$$4(s_0^2-l\omega s_0+l^2)-(2s_0-l\omega)^2=l^2(4-\omega^2)\equiv 0 \bmod \mathfrak{p}.$$

Since $\omega+2\in\mathcal{O}_k^\times$, it holds that $\mathfrak{p}=(\omega-2)$, a contradiction. Hence, the congruence $s^2-l\omega s+l^2\equiv 0 \bmod \mathfrak{p}^2$ has at most two solutions on $\mathcal{O}_k/\mathfrak{p}^2$.

Let $\mathfrak{p}=(\omega-2)$. Then it is easily checked that the solutions of $s^2-l\omega s+l^2\equiv 0 \bmod \mathfrak{p}^2$ are $0+t(\omega-2)$ in $\mathcal{O}_k/\mathfrak{p}^2$ ($t\in\mathcal{O}_k/\mathfrak{p}\simeq\mathbb{Z}/l\mathbb{Z}$). □

Lemma 3.5.5. *Let l be an odd prime number and $k=\mathbb{Q}(\omega)$. Let $\mathfrak{p}$ be a prime ideal of k. Then we have*

$$\sum_{\mathfrak{p}\nmid(l)}\frac{1}{N(\mathfrak{p})^2}\leq\frac{2l^2}{(l+1)^2(l-1)}$$

where $\mathfrak{p}$ runs through prime ideals of k except for $\mathfrak{p}\mid(l)$ and N denotes the absolute norm of k.

Proof. We easily have

$$\sum_{\mathfrak{p}\nmid(l)}\frac{1}{N(\mathfrak{p})^2}\leq[k:\mathbb{Q}]\sum_{p\neq l}\frac{1}{(p^{f_p})^2}=\frac{l-1}{2}\sum_{p\neq l}\frac{1}{(p^{f_p})^2}$$

where p runs through the prime numbers except for l. If $p \neq l$, f_p is equal to the minimal positive integer f satisfying $p^f \equiv \pm 1 \bmod l$ because p is unramified in k and $\mathrm{Gal}(k/\mathbb{Q}) \simeq (\mathbb{Z}/l\mathbb{Z})^\times/\{\pm 1\}$. Hence we have

$$\begin{aligned}
\frac{l-1}{2}\sum_{p\neq l}\frac{1}{(p^{f_p})^2} &\leq \frac{l-1}{2}\sum_{k=1}^{\infty}\left\{\frac{1}{(kl+1)^2}+\frac{1}{(kl-1)^2}\right\} \\
&= \frac{l-1}{2}\left\{\frac{1}{(l+1)^2}+\frac{1}{(l-1)^2}+\sum_{k=2}^{\infty}\frac{1}{(kl+1)^2}+\frac{1}{(kl-1)^2}\right\} \\
&\leq \frac{l-1}{2}\left\{\frac{1}{(l+1)^2}+\frac{1}{(l-1)^2}+\int_{x=1}^{\infty}\frac{1}{(lx+1)^2}+\frac{1}{(lx-1)^2}dx\right\} \\
&= \frac{l-1}{2}\left\{\frac{1}{(l+1)^2}+\frac{1}{(l-1)^2}+\frac{1}{l(l+1)}+\frac{1}{l(l-1)}\right\} \\
&= \frac{2l^2}{(l+1)^2(l-1)}.
\end{aligned}$$

The assertion is clear. □

Acknowledgments

First of all, I would like to express my sincere gratitude to my supervisor Professor Tomokazu Kashio for his continuing support in this study. He always provided me helpful comments and considerable encouragement. This thesis is not the same without his support.

I would also like to express my profound gratitude to my former supervisor Professor Yoshitaka Hachimori for his enormous help. I have been able to continue this research with his support.

I am deeply thankful to the members of the thesis committee, Professor Hiroyuki Ito, Professor Susumu Hirose, Professor Kazuko Matsumoto, Professor Nobuko Miyamoyo, and Professor Masanari Kida for incisive comments. Their comments make this thesis much better than the previous version.

Furthermore I would like to thank many people who have discussed and commented on this study.

Finally, I am grateful to my family for their understanding and support.

Bibliography

[1] Archinard, G., Extensions cubiques cycliques de $\mathbb{Q}$ dont l'anneau des entiers est monogène, *Enseign. Math. (2).* **20** (1974), 179–203.

[2] Cusick, T.W., Lower bounds for regulators. Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), *Lecture Notes in Math.*, **1068** (1984), 63–73.

[3] Dedekind, R., Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Abh.-Akad. Wiss. Goettin. Math. Phys. Kl.* **23** (1878), 1–23.

[4] Dummit, D.S., Kisilevsky, H., Indices in cyclic cubic fields. *Number theory and algebra*, Academic Press, New York, (1977), 29–42.

[5] Foster, K., HT90 and "simplest" number fields, *Illinois Journal of Mathematics* **55** (2011), no. 4, 1621–1655.

[6] Gras, M.-N., Sur les corps cubiques cycliques dont l'anneau des entiers est-monogène, *Ann. Sci. Univ. Besançon Math. (3)*, No. 6 (1973), 26 pp.

[7] Gras, M.-N., Sur les corps cubiques cycliques dont l'anneau des entiers est-monogène, *C. R. Acad. Sci. Paris Sér. A* **278** (1974), 59–62.

[8] Gras, M.-N., Lien entre le groupe des unités et la monogèneité des corps cubiques cycliques, *Séminaire de Théorie des Nombres Besançon*, Année 1975-76.

[9] Gras, M.-N., Non monogènéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geqq 5$, *J. Number Theory* **23** (1986), no. 3, 347–353.

[10] Hoshi, A., On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the simplest cubic fields, *J. Number Theory* **131** (2011), no. 11, 2135–2150.

[11] Kashio, T., Sekigawa, R., The characterization of cyclic cubic fields with power integral bases, *Kodai Math. J.* **44** (2021), no. 2, 290–306.

[12] Komatsu, T., Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory, *Manuscripta Math.* **114** (2004), 265–279.

[13] Nakahara, T., On the minimum index of a cyclic quartic field, *Arch. Math.* **48** (1987), 322–325.

[14] Nakahara, T., Hasse's problem for monogenic fields, *Ann. Math. Blaise Pascal* **16** (2009), no. 1, 47–56.

[15] Okazaki, R., The simplest cubic fields are non-isomorphic to each other, in preparation.

[16] Rikuna, Y., On simple families of cyclic polynomials, *Proc. Amer. Math. Soc.* **130** (2002), 2215–2218.

[17] Schertz, R., Complex multiplication, *New Math. Monogr.* **15**, Cambridge University Press, Cambridge (2010).

[18] Sekigawa, R., Relative power integral bases in certain ray class fields of an imaginary quadratic number field, preprint.

[19] Sekigawa, R., Rikuna's generic cyclic polynomial and the monogenity, *J. Number Theory* **231** (2022), 239–250.

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

[21] Shintani, T., On evaluation of zeta functions of totally real algebraic number fields at non-positive integer, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **23** (1976), no. 2, 393–417.

[22] Yokoi, H., On the class number of a relatively cyclic number field, *Nagoya Math. J.* **29** (1967), 31–44.