

# *Mathematical Journal of Okayama University*

---

*Volume 47, Issue 1*

2005

*Article 1*

JANUARY 2005

---

## The Spiegelungssatz for $p=5$ from a Constructive Approach

Yasuhiro Kishi\*

\*Fukuoka University of Education

Copyright ©2005 by the authors. *Mathematical Journal of Okayama University* is produced by  
The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

# The Spiegelungssatz for $p=5$ from a Constructive Approach

Yasuhiro Kishi

## Abstract

We describe explicitly the relation between the 5-ranks of the ideal class groups of two quadratic fields with conductors  $m$  and  $5m$ , respectively, and that of the associated cyclic quartic field.

**KEYWORDS:** Class Groups, Quadratic Fields, Quartic Fields

Math. J. Okayama Univ. **47** (2005), 1–27

# THE SPIEGELUNGSSATZ FOR $p = 5$ FROM A CONSTRUCTIVE APPROACH

YASUHIRO KISHI

ABSTRACT. We describe explicitly the relation between the 5-ranks of the ideal class groups of two quadratic fields with conductors  $m$  and  $5m$ , respectively, and that of the associated cyclic quartic field.

## 1. INTRODUCTION

The “Spiegelungssatz” gives the relation between the  $p$ -ranks of the ideal class groups of two different number fields. The first “Spiegelungssatz” was given by Scholz [10] in 1932 for  $p = 3$ . He gave a relation between the 3-rank of the ideal class group of an imaginary quadratic field  $\mathbb{Q}(\sqrt{d})$  and that of the associated real quadratic field  $\mathbb{Q}(\sqrt{-3d})$ : Let  $r$  denote the former and  $s$  the latter. Then we have the inequalities  $s \leq r \leq s + 1$ . Some extensions were given by several authors; for example, Leopoldt [6], Kuroda [5], and recently Gras [2]. According to them, the associated field of a quadratic field for  $p = 5$  is a cyclic quartic field. Moreover, the associated field of  $\mathbb{Q}(\sqrt{d})$  and that of  $\mathbb{Q}(\sqrt{5d})$  are the same. In the present paper, we extend Scholz’s inequalities to  $p = 5$  by constructing polynomials with data of  $\mathbb{Q}(\sqrt{d})$  and  $\mathbb{Q}(\sqrt{5d})$  which generate unramified cyclic quintic extensions of the associated quartic field; as a consequence, we describe explicitly the relation between the 5-ranks of the ideal class groups of  $\mathbb{Q}(\sqrt{d})$  and  $\mathbb{Q}(\sqrt{5d})$ , and that of the associated quartic field.

Let  $d (\neq 1)$  be a square free integer prime to 5, and let  $\zeta$  be a primitive fifth root of unity. We define two quadratic fields  $k_1 = \mathbb{Q}(\sqrt{d})$  and  $k_2 = \mathbb{Q}(\sqrt{5d})$ . Then there exists a unique proper subextension of the bicyclic biquadratic extension  $k_1(\zeta)/\mathbb{Q}(\sqrt{5})$  other than  $k_1(\sqrt{5})$  and  $\mathbb{Q}(\zeta)$ . We denote it by  $M$ . Then  $M$  is a cyclic quartic field, and  $M(\zeta)$  coincides with  $k_1(\zeta)$ .

Let  $\text{Cl}(k_i)$  be the ideal class group of  $k_i$ , and let  $\text{Syl}_5^{\text{el}}\text{Cl}(k_i)$  denote the elementary Sylow 5-subgroup of  $\text{Cl}(k_i)$ . Moreover, let  $r_i$  be the 5-rank of  $\text{Cl}(k_i)$ . Then we can express

$$\text{Syl}_5^{\text{el}}\text{Cl}(k_i) = \langle [\mathfrak{a}_{i1}] \rangle \times \cdots \times \langle [\mathfrak{a}_{ir_i}] \rangle,$$

where  $\mathfrak{a}_{ij}$ ,  $1 \leq j \leq r_i$ , are non-principal prime ideals of  $k_i$  of degree 1 and prime to 5. Then  $\mathfrak{a}_{ij}^5$  is principal. Fix an integer  $\alpha_{ij} \in \mathcal{O}_{k_i}$  with  $(\alpha_{ij}) = \mathfrak{a}_{ij}^5$

---

This research was partially supported by JSPS Research Fellowships for Young Scientists.

for each  $j$ ;  $\alpha_{ij}$  is not a fifth power in  $k_i$ . We define the sets  $S(k_i)$  ( $i = 1, 2$ ) as follows:

$$S(k_i) := \begin{cases} \{\alpha_{ij} \mid 1 \leq j \leq r_i\} \cup \{\varepsilon_i\} & \text{if } d > 0, \\ \{\alpha_{ij} \mid 1 \leq j \leq r_i\} & \text{if } d < 0, \end{cases}$$

where  $\varepsilon_i$  is the fundamental unit of  $k_i$ , if  $d > 0$ .

For  $\alpha \in \mathcal{O}_{k_1}$  and for  $\beta \in \mathcal{O}_{k_2}$ , we define six conditions, (A-i) through (A-v) and (B), as follows:

$$(A-i) \quad \text{Tr}_{k_1}(\alpha)^2 \equiv 4N_{k_1}(\alpha) \pmod{5^3};$$

$$(A-ii) \quad \text{Tr}_{k_1}(\alpha) \equiv 0 \pmod{5^2};$$

$$(A-iii) \quad \text{Tr}_{k_1}(\alpha)^2 \equiv N_{k_1}(\alpha) \pmod{5^2};$$

$$(A-iv) \quad \text{Tr}_{k_1}(\alpha)^2 \equiv 2N_{k_1}(\alpha) \pmod{5^2};$$

$$(A-v) \quad \text{Tr}_{k_1}(\alpha)^2 \equiv 3N_{k_1}(\alpha) \pmod{5^2};$$

$$(B) \quad \text{Tr}_{k_2}(\beta)^2 \equiv 4N_{k_2}(\beta) \pmod{5^2},$$

where  $N_{k_i}$  and  $\text{Tr}_{k_i}$  are the norm map and the trace map of  $k_i/\mathbb{Q}$ , respectively. Under the above notation, we define  $\delta_1$  and  $\delta_2$  respectively by

$$\delta_1 := \begin{cases} 1 & \text{if none of the five conditions (A-i) through (A-v)} \\ & \text{holds for some } \alpha \in S(k_1), \\ 0 & \text{if one of the five conditions (A-i) through (A-v)} \\ & \text{holds for every } \alpha \in S(k_1), \end{cases}$$

$$\delta_2 := \begin{cases} 1 & \text{if the condition (B) does not hold for some } \beta \in S(k_2), \\ 0 & \text{if the condition (B) holds for every } \beta \in S(k_2). \end{cases}$$

**Main Theorem.** *Let the notation be as above. Moreover let  $r$  be the 5-rank of the ideal class group of  $M$ . Then we have*

$$r = \begin{cases} r_1 + r_2 + 2 - \delta_1 - \delta_2 & \text{if } d > 0, \\ r_1 + r_2 - \delta_1 - \delta_2 & \text{if } d < 0. \end{cases}$$

*Remark 1.1.* (1) The set  $S(k_i)$  depends on the choice of generators of  $\text{Syl}_5^{\text{el}}\text{Cl}(k_i)$ . However,  $\delta_i$  does not so (cf. Proposition 5.1).

(2) Case (A-iv) occurs only when  $d \equiv \pm 1 \pmod{5}$ , and cases (A-iii), (A-v) occur only when  $d \equiv \pm 2 \pmod{5}$  (cf. Proposition 5.5).

*Remark 1.2.* It follows from known results; for example, [11, Section 10] and [2, Théorème 7.7], and so on, that the difference between  $r$  and  $r_1 + r_2$  is at most equal to 2.

For our proof of the main theorem, we give all of those unramified cyclic quintic extensions of  $M$  which are  $F_5$ -extensions of  $\mathbb{Q}$ , by constructing quintic polynomials with rational coefficients. Here for an odd prime  $p$  in general,  $F_p$  denotes the Frobenius group of order  $p(p-1)$ :

$$F_p = \langle \sigma, \iota \mid \sigma^p = \iota^{p-1} = 1, \iota^{-1}\sigma\iota = \sigma^a \rangle,$$

where  $a$  is a primitive root modulo  $p$ . According to class field theory,  $\text{Syl}_5^{\text{el}}\text{Cl}(M)$  is isomorphic to the Galois group of the composite field of all unramified cyclic quintic extensions of  $M$  over  $M$ . However, in Section 2 we show that the 5-rank of  $\text{Cl}(M)$  can be calculated by considering only unramified cyclic quintic extensions of  $M$  which are  $F_5$ -extensions of  $\mathbb{Q}$ . In Section 3, we study  $F_p$ -polynomials for a general odd prime  $p$ . By applying Section 3 to the case  $p = 5$ , we construct unramified cyclic quintic extensions of  $M$  which are  $F_5$ -extensions of  $\mathbb{Q}$  in Section 4. In Section 5, we finish the proof of the main theorem. As an application of our main theorem, we give another proof of Parry's result on the 5-divisibility of the class number of a certain imaginary cyclic quartic field in Section 6. We give in the last Section 7, some numerical examples.

## 2. CLASSIFICATION OF UNRAMIFIED CYCLIC QUINTIC EXTENSIONS

In this section, we will use the same notation as in Section 1.

Fix a generator  $\rho$  of  $\text{Gal}(M(\zeta)/k_1)$ , and assume that  $\zeta^\rho = \zeta^2$ . We classify unramified cyclic quintic extensions  $E$  of  $M$  into the following three types:

- (i)  $E/\mathbb{Q}$  is normal and its Galois group is

$$\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \iota \mid \sigma^5 = \iota^4 = 1, \iota^{-1}\sigma\iota = \sigma^2 \rangle$$

with  $\iota|_M = \rho|_M$ ;

- (ii)  $E/\mathbb{Q}$  is normal and its Galois group is

$$\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \iota \mid \sigma^5 = \iota^4 = 1, \iota^{-1}\sigma\iota = \sigma^3 \rangle$$

with  $\iota|_M = \rho|_M$ ;

- (iii)  $E/\mathbb{Q}$  is not normal.

*Remark 2.1.* As is observed in [7], every unramified cyclic quintic extension of  $M$  is normal over  $\mathbb{Q}(\sqrt{5})$ . From the fact that the only primitive roots modulo 5 are 2 and 3, and the fact that the class number of  $\mathbb{Q}(\sqrt{5})$  is not divisible by 5, every unramified cyclic quintic extension of  $M$  satisfies one of the above three conditions.

**Definition 2.2.** An unramified cyclic quintic extension  $E$  of  $M$  is said to be of *Type (I)*, *(II)* or *(III)* if  $E$  satisfies the condition (i), (ii) or (iii), respectively.

**Proposition 2.3.** *Let  $E$  be an unramified cyclic quintic extension of  $M$  of Type (III). Then there exist unramified cyclic quintic extensions  $E_1/M$  and  $E_2/M$  of Type (I) and Type (II), respectively, so that we have  $E \subset E_1 E_2$ .*

For our proof of this proposition we need the following two lemmas.

**Lemma 2.4.** *Let  $E$  be an unramified cyclic quintic extension of  $M$ . If  $E$  is of Type (III), then the Galois closure of  $E$  over  $\mathbb{Q}$  is of degree 100, and has two subfields of degree 20 which are normal over  $\mathbb{Q}$ .*

*Proof.* Assume that  $E$  is of Type (III). Since  $E/M$  is an unramified extension,  $E$  is normal over  $\mathbb{Q}(\sqrt{5})$ . Let  $h(X) \in \mathbb{Q}(\sqrt{5})[X]$  be a polynomial of degree 5 which generates  $E$  over  $\mathbb{Q}(\sqrt{5})$ . Since  $E/\mathbb{Q}$  is not normal, we have  $h(X) \notin \mathbb{Q}[X]$ . Let  $\nu$  be a generator of  $\text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ . Then  $h^\nu(X)$  is irreducible over  $\mathbb{Q}(\sqrt{5})$ . Denote the minimal splitting field of  $h^\nu(X)$  over  $\mathbb{Q}(\sqrt{5})$  by  $E'$ . Then  $EE'$  is the minimal splitting field of  $h(X)h^\nu(X)$  over  $\mathbb{Q}(\sqrt{5})$ . Since  $h(X)h^\nu(X) \in \mathbb{Q}[X]$ ,  $EE'/\mathbb{Q}$  is normal. Hence the Galois closure  $\overline{E}$  of  $E$  over  $\mathbb{Q}$  is contained in  $EE'$ . On the other hand,  $E'$  contains  $M$  because  $M/\mathbb{Q}$  is normal. Since  $E'/\mathbb{Q}(\sqrt{5})$  is normal,  $E'$  is a cyclic quintic extension of  $M$ . Hence  $EE'$  is a bicyclic biquintic extension of  $M$ ; that is,  $\text{Gal}(EE'/M) \simeq C_5 \times C_5$ . Since the extension  $EE'/E$  has no proper subfield,  $EE'$  coincides with  $\overline{E}$ . Then we have

$$[\overline{E} : \mathbb{Q}] = [\overline{E} : M][M : \mathbb{Q}] = 25 \cdot 4 = 100.$$

Let us write  $G = \text{Gal}(\overline{E}/\mathbb{Q})$  for simplicity. Let  $H_1 := \langle \sigma_1 \rangle$  and  $H_2 := \langle \sigma_2 \rangle$  be the subgroups of  $G$  corresponding to  $E$  and  $E'$ , respectively, and put  $A := H_1 \times H_2$ . Moreover, let  $B := \langle \iota \rangle$  be the subgroup of  $G$  of order 4. By  $(|A|, |B|) = 1$ , we have

$$G = AB = \langle \sigma_1, \sigma_2, \iota \rangle.$$

We now consider a subgroup  $\text{Gal}(\overline{E}/\mathbb{Q}(\sqrt{5}))$  of  $G$ . Since  $E$  and  $E'$  are both  $D_5$ -extensions of  $\mathbb{Q}(\sqrt{5})$ , we can express

$$\text{Gal}(\overline{E}/\mathbb{Q}(\sqrt{5})) = \left\langle \sigma_1, \sigma_2, \iota^2 \left| \begin{array}{l} \sigma_1^5 = \sigma_2^5 = (\iota^2)^2 = 1, \sigma_1 \sigma_2 = \sigma_2 \sigma_1, \\ \iota^{-2} \sigma_1 \iota^2 = \sigma_1^{-1}, \iota^{-2} \sigma_2 \iota^2 = \sigma_2^{-1} \end{array} \right. \right\rangle.$$

Since  $E^\iota = E'$ , we get

$$(E')^{\iota^{-1} \sigma_1 \iota} = E^{\sigma_1 \iota} = E^\iota = E'.$$

Therefore, we have  $\iota^{-1} \sigma_1 \iota = \sigma_2^x$  for some  $x$ ,  $1 \leq x \leq 4$ . With replacement of a generator  $\sigma_2$ , we may assume  $x = 1$ . In a similar way, we get  $\iota^{-1} \sigma_2 \iota = \sigma_1^y$  for some  $y$ ,  $1 \leq y \leq 4$ . Then we have

$$\sigma_1^{-1} = \iota^{-2} \sigma_1 \iota^2 = \iota^{-2} (\iota \sigma_2 \iota^{-1}) \iota^2 = \iota^{-1} \sigma_2 \iota = \sigma_1^y,$$

and hence  $y = 4$ . From this, we see that  $\langle \sigma_1 \sigma_2^2 \rangle$  and  $\langle \sigma_1 \sigma_2^3 \rangle$  are both normal subgroups of  $G$ . Indeed, we have

$$\begin{aligned}\iota^{-1}(\sigma_1 \sigma_2^2) \iota &= \sigma_2 \iota^{-1} \iota \sigma_1^{-2} = \sigma_1^3 \sigma_2 = (\sigma_1 \sigma_2^2)^3, \\ \iota^{-1}(\sigma_1 \sigma_2^3) \iota &= \sigma_2 \iota^{-1} \iota \sigma_1^{-3} = \sigma_1^2 \sigma_2 = (\sigma_1 \sigma_2^3)^2.\end{aligned}$$

Then the two subfields of  $\overline{E}$  corresponding to  $\langle \sigma_1 \sigma_2^2 \rangle$  and  $\langle \sigma_1 \sigma_2^3 \rangle$  are normal over  $\mathbb{Q}$  and of degree 20. The proof is completed.  $\square$

**Lemma 2.5.** *Let  $E_1$  and  $E_2$  be unramified cyclic quintic extensions of  $M$ . If both of them are of Type (I) (resp. of Type (II)), then all proper subextensions of  $E_1 E_2 / M$  are of Type (I) (resp. of Type (II)).*

*Proof.* We note that all proper subextensions of  $E_1 E_2 / M$  are unramified cyclic quintic extensions of  $M$ .

Now express

$$\text{Gal}(E_1 E_2 / \mathbb{Q}) = \langle \sigma_1, \sigma_2, \iota \mid \sigma_1^5 = \sigma_2^5 = \iota^4 = 1, \sigma_1 \sigma_2 = \sigma_2 \sigma_1 \rangle$$

with  $\iota|_M = \rho|_M$  and let  $\langle \sigma_1 \rangle$  and  $\langle \sigma_2 \rangle$  be the subgroups of  $\text{Gal}(E_1 E_2 / \mathbb{Q})$  corresponding to  $E_1$  and  $E_2$ , respectively. Then we have

$$\text{Gal}(E_1 / \mathbb{Q}) = \langle \sigma_2|_{E_1}, \iota|_{E_1} \rangle \quad \text{and} \quad \text{Gal}(E_2 / \mathbb{Q}) = \langle \sigma_1|_{E_2}, \iota|_{E_2} \rangle.$$

Hence by the assumption, the relations  $\iota^{-1} \sigma_1 \iota = \sigma_1^l$  and  $\iota^{-1} \sigma_2 \iota = \sigma_2^l$  hold, where  $l = 2$  or  $3$  according to whether  $E_1$  and  $E_2$  are of Type (I) or of Type (II). Note that every proper subextension of  $E_1 E_2 / M$  except for  $E_1$  and  $E_2$  corresponds to a subgroup  $\langle \sigma_1^j \sigma_2 \rangle$  of  $\text{Gal}(E_1 E_2 / \mathbb{Q})$  for some  $j$ ,  $1 \leq j \leq 4$ . Since

$$\iota^{-1}(\sigma_1^j \sigma_2) \iota = (\iota^{-1} \sigma_1^j \iota)(\iota^{-1} \sigma_2 \iota) = (\iota^{-1} \sigma_1 \iota)^j (\iota^{-1} \sigma_2 \iota) = (\sigma_1^l)^j \sigma_2^l = (\sigma_1^j \sigma_2)^l,$$

we obtain the desired conclusion.  $\square$

*Proof of Proposition 2.3.* Let  $E$  be an unramified cyclic quintic extension of  $M$  of Type (III), and let  $\tau$  be an automorphism of  $E/\mathbb{Q}$  of order 2. Since  $M$  is normal over  $\mathbb{Q}$ ,  $E^\tau$  contains  $M$ . By using Lemma 2.4, the Galois closure  $\overline{E}$  of  $E$  over  $\mathbb{Q}$  has two subfields of degree 20 which are normal over  $\mathbb{Q}$ . We denote them by  $E_1$  and  $E_2$ . It is clear that  $\overline{E} = EE^\tau = E_1 E_2$ . Since  $E$  and  $E^\tau$  are both unramified over  $M$ , so is  $\overline{E}$ . Then  $E_1$  and  $E_2$  are both unramified over  $M$  also. By using Lemma 2.5, one is of Type (I) and the other is of Type (II).  $\square$

Let  $\overline{E}_1$  (resp.  $\overline{E}_2$ ) be the composite field of all unramified cyclic quintic extensions of  $M$  of Type (I) (resp. of Type (II)). Then by using Lemma 2.5, we have

$$(2.1) \quad \overline{E}_1 \cap \overline{E}_2 = M.$$

Put  $\overline{E} := \overline{E}_1 \overline{E}_2$ . It is clear that  $\overline{E}$  is unramified over  $M$  and contains all unramified cyclic quintic extensions of  $M$  of Types (I) or (II). Let  $E_3$  be an unramified cyclic quintic extension of  $M$  of Type (III). Then by Proposition 2.3, we have  $E_3 \subset \overline{E}_1 \overline{E}_2 = \overline{E}$ . Hence the composite field of all unramified cyclic quintic extensions of  $M$  coincides with  $\overline{E}$ . From this, together with (2.1), we can prove

$$(2.2) \quad \mathrm{Syl}_5^{\mathrm{el}} \mathrm{Cl}(M) \simeq \mathrm{Gal}(\overline{E}/M) \simeq \mathrm{Gal}(\overline{E}_1/M) \times \mathrm{Gal}(\overline{E}_2/M).$$

We see therefore that the 5-rank of  $\mathrm{Cl}(M)$  can be calculated by considering only unramified cyclic quintic extensions of  $M$  of Types (I) and (II).

### 3. $F_p$ -EXTENSIONS OF THE RATIONAL NUMBER FIELD

First we review a part of Imaoka and the author's work in [4].

Let  $p$  be an odd prime and let  $\zeta$  be a primitive  $p$ -th root of unity. Let  $k$  be a quadratic field different from  $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ . Then there exists a unique proper subextension of the bicyclic biquadratic extension  $k(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})$  other than  $k(\zeta + \zeta^{-1})$  and  $\mathbb{Q}(\zeta)$ . We denote it by  $M$ . Then  $M$  is a cyclic field of degree  $p-1$ .

Fix a generator  $\tau$  of  $\mathrm{Gal}(M(\zeta)/M)$ . We define subsets  $\mathcal{M}(M)$  and  $\mathcal{N}(M)$  of  $M(\zeta)^\times$  as follows:

$$\begin{aligned} \mathcal{M}(M) &:= \{\gamma \in M(\zeta)^\times \mid \gamma^{-1+\tau} \notin M(\zeta)^p\}, \\ \mathcal{N}(M) &:= M(\zeta)^\times \setminus \mathcal{M}(M). \end{aligned}$$

For  $\alpha \in k$ , we define the polynomial  $f_p(X; \alpha)$  by

$$f_p(X; \alpha) := \sum_{i=0}^{(p-1)/2} (-N(\alpha))^i \frac{p}{p-2i} \binom{p-i-1}{i} X^{p-2i} - N(\alpha)^{(p-1)/2} \mathrm{Tr}(\alpha),$$

where  $N$  and  $\mathrm{Tr}$  are the norm map and the trace map of  $k/\mathbb{Q}$ . Denote the minimal splitting field of  $f_p(X; \alpha)$  over  $\mathbb{Q}$  by  $K_\alpha$ .

**Proposition 3.1** ([4, Theorem 2.1, Corollary 2.6]). *Let the notation be as above. Fix a generator  $\rho$  of  $\mathrm{Gal}(M(\zeta)/k)$ , and take an element  $l(\rho) \in \mathbb{Z}$  so that we have  $\zeta^\rho = \zeta^{l(\rho)}$ . Then for  $\alpha \in \mathcal{M}(M) \cap k$ ,  $K_\alpha$  is an  $F_p$ -extension of  $\mathbb{Q}$  containing  $M$ . Furthermore, let  $\sigma$  and  $\iota$  be generators of  $\mathrm{Gal}(K_\alpha/\mathbb{Q})$  which satisfy the following two relations:*

- (i)  $\iota|_M = \rho|_M$ ;
- (ii)  $\sigma^p = \iota^{p-1} = 1$ .

Then we have

$$\iota^{-1} \sigma \iota = \sigma^{l(\rho)}.$$



Conversely, every Galois extension  $E$  of  $\mathbb{Q}$  containing  $M$  with Galois group

$$\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \iota \mid \sigma^p = \iota^{p-1} = 1, \iota^{-1}\sigma\iota = \sigma^{l(\rho)} \rangle,$$

where  $\iota|_M = \rho|_M$ , is given as  $E = K_\alpha$  for some  $\alpha \in \mathcal{M}(M) \cap k$ .

A criterion for two fields  $K_{\alpha_1}$  and  $K_{\alpha_2}$  with  $\alpha_1, \alpha_2 \in \mathcal{M}(M) \cap k$  to coincide with each other is given by the following proposition.

**Proposition 3.2** ([4, Proposition 1.3]). *For elements  $\alpha_1, \alpha_2 \in \mathcal{M}(M) \cap k$ , the following statements are equivalent:*

- (a)  $K_{\alpha_1} = K_{\alpha_2}$ ;
- (b)  $\alpha_1^n / \alpha_2 \in \mathcal{N}(M)$  for some  $n \in \mathbb{Z} \setminus p\mathbb{Z}$ .

*Remark 3.3.* It follows from this proposition that we may replace  $\mathcal{M}(M) \cap k$  by  $\mathcal{M}(M) \cap \mathcal{O}_k$  in the statement of Proposition 3.1.

Next we show the following proposition with respect to the ramification. For a prime number  $p$  and for an integer  $m$ , we denote by  $v_p(m)$  the greatest exponent  $\mu$  of  $p$  such that  $p^\mu \mid m$ .

**Proposition 3.4.** *Let  $q$  be a prime and  $\theta$  be a root of  $f_p(X; \alpha)$  for  $\alpha \in \mathcal{M}(M) \cap \mathcal{O}_k$ . Assume that  $(N(\alpha), \text{Tr}(\alpha)) = 1$ . Then the condition*

$$v_q(N(\alpha)) \not\equiv 0 \pmod{p}$$

*is a sufficient condition for the prime  $q$  to be totally ramified in  $\mathbb{Q}(\theta)$ . Moreover, if  $q \neq p$ , it is also necessary.*

For the proof of this proposition, we need the following Sase's results.

**Proposition 3.5** ([9, Proposition 2]). *Let  $p (\neq 2)$  and  $q$  be prime numbers. Suppose that the polynomial*

$$\varphi(X) = X^p + \sum_{j=0}^{p-2} a_j X^j, \quad a_j \in \mathbb{Z}$$

*is irreducible over  $\mathbb{Q}$  and satisfies the condition*

$$(3.1) \quad v_q(a_j) < p - j \quad \text{for some } j, 0 \leq j \leq p - 2.$$

*Let  $\theta$  be a root of  $\varphi(X)$ .*

(1) *If  $q$  is different from  $p$ , then  $q$  is totally ramified in  $\mathbb{Q}(\theta)/\mathbb{Q}$  if and only if*

$$0 < \frac{v_q(a_0)}{p} \leq \frac{v_q(a_j)}{p - j} \quad \text{for every } j, 1 \leq j \leq p - 2.$$

(2) The prime  $p$  is totally ramified in  $\mathbb{Q}(\theta)/\mathbb{Q}$  if and only if one of the following conditions (S-i), (S-ii) holds:

$$(S-i) \quad 0 < \frac{v_p(a_0)}{p} \leq \frac{v_p(a_j)}{p-j} \quad \text{for every } j, 1 \leq j \leq p-2;$$

$$(S-ii) \quad (S-ii-1) \quad v_p(a_0) = 0,$$

$$(S-ii-2) \quad v_p(a_j) > 0 \quad \text{for every } j, 1 \leq j \leq p-2,$$

$$(S-ii-3) \quad \frac{v_p(\varphi(-a_0))}{p} \leq \frac{v_p(\varphi^{(j)}(-a_0))}{p-j} \quad \text{for every } j, 1 \leq j \leq p-2,$$

and

$$(S-ii-4) \quad v_p(\varphi^{(j)}(-a_0)) < p-j \quad \text{for some } j, 0 \leq j \leq p-1,$$

where  $\varphi^{(j)}(X)$  is the  $j$ -th differential of  $\varphi(X)$ .

*Proof of Proposition 3.4.* Let  $\alpha$  be an element of  $\mathcal{M}(M) \cap \mathcal{O}_k$ . It follows from Proposition 3.1 that  $f_p(X; \alpha)$  is irreducible over  $\mathbb{Q}$ . Let  $q$  be a prime number. Express

$$v_q(N(\alpha)^{(p-1)/2}) = pu + v, \quad u, v \in \mathbb{Z}, \quad 0 \leq v \leq p-1, \quad u \geq 0,$$

and put

$$N(\alpha) = q^{2(pu+v)/(p-1)}w, \quad w \in \mathbb{Z}, \quad q \nmid w.$$

Then we have

$$\begin{aligned} f_p(X; \alpha) &= \sum_{i=0}^{(p-1)/2} (-q^{2(pu+v)/(p-1)}w)^i \frac{p}{p-2i} \binom{p-i-1}{i} X^{p-2i} \\ &\quad - q^{pu+v}w^{(p-1)/2}\text{Tr}(\alpha). \end{aligned}$$

Divide both sides of this equation by  $q^{pu}$ , and put  $X = q^u Y$ ; then we have

$$\begin{aligned} g_p(Y; \alpha) &:= \frac{f_p(q^u Y; \alpha)}{q^{pu}} \\ &= \sum_{i=0}^{(p-1)/2} q^{2i(u+v)/(p-1)}(-w)^i \frac{p}{p-2i} \binom{p-i-1}{i} Y^{p-2i} \\ &\quad - q^v w^{(p-1)/2}\text{Tr}(\alpha). \end{aligned}$$

Since

$$0 \leq \frac{2(u+v)}{p-1} = \frac{2(pu+v)}{p-1} - 2u \in \mathbb{Z},$$

we have  $g_p(Y; \alpha) \in \mathbb{Z}[Y]$ . Let denote the coefficient of  $Y^j$  in  $g_p(Y; \alpha)$  by  $a_j$ . When  $q \nmid N(\alpha)$ , we have  $v_q(a_1) = 0$  or  $1$  according to whether  $q$  is equal to  $p$  or not; and hence  $v_q(a_1) < p-1$ . When  $q \mid N(\alpha)$ , we have  $v_q(a_0) = v < p$

because  $(N(\alpha), \text{Tr}(\alpha)) = 1$ . Therefore,  $g_p(Y; \alpha)$  satisfies the condition (3.1) in any case. Hence we can apply Proposition 3.5 to  $g_p(Y; \alpha)$ .

Assume that  $v_q(N(\alpha)) \not\equiv 0 \pmod{p}$ . Then we have  $v_q(\text{Tr}(\alpha)) = 0$  by the assumption. Let us show the inequality

$$(3.2) \quad 0 < \frac{v_q(a_0)}{p} \leq \frac{v_q(a_j)}{p-j} \quad \text{for every } j, 1 \leq j \leq p-2.$$

Since  $v \neq 0$ , the first inequality of the condition (3.2) holds. We see that, for every  $j$ ,  $1 \leq j \leq p-2$ ,

$$\begin{aligned} \frac{v_q(a_j)}{p-j} - \frac{v_q(a_0)}{p} &\geq \frac{\frac{2(u+v)}{p-1} \cdot \frac{p-j}{2} + \varepsilon}{p-j} - \frac{v}{p} \\ &= \frac{pu+v}{p(p-1)} + \frac{\varepsilon}{p-j} \\ &> 0; \end{aligned}$$

here  $\varepsilon = 1$  or  $0$  according to whether  $q$  is equal to  $p$  or not. Hence the second inequality of (3.2) also holds. Therefore,  $q$  is totally ramified in  $\mathbb{Q}(\theta)$ .

Assume that  $q \neq p$  and  $v_q(N(\alpha)) \equiv 0 \pmod{p}$ . In this case, the inequality (3.2) does not hold. Indeed, we have  $a_{p-2} = -pw \not\equiv 0 \pmod{q}$  because  $v = 0$ , if  $q \nmid N(\alpha)$ , and  $a_0 = w^{(p-1)/2} \text{Tr}(\alpha) \not\equiv 0 \pmod{q}$  because  $(N(\alpha), \text{Tr}(\alpha)) = 1$ , if  $q \mid N(\alpha)$ . Therefore,  $q$  is not totally ramified in  $\mathbb{Q}(\theta)$ . The proof is completed.  $\square$

#### 4. CONSTRUCTION OF UNRAMIFIED CYCLIC QUINTIC EXTENSIONS

In this section, we apply the previous section to the case  $p = 5$ .

Let  $\zeta$  be a primitive fifth root of unity, and let  $k = \mathbb{Q}(\sqrt{D})$  be a quadratic field, where  $D$  is a square free integer and is different from 5. Let  $M$  be the same definition as in Section 3; then  $M$  is a cyclic quartic field containing  $\mathbb{Q}(\sqrt{5})$ . Fix a generator  $\rho$  of  $\text{Gal}(M(\zeta)/k)$ , and take an element  $l(\rho) \in \mathbb{Z}$  so that we have  $\zeta^\rho = \zeta^{l(\rho)}$ . Moreover, we define subsets  $\mathcal{M}_5(M)$  and  $\mathcal{N}_5(M)$  of  $M(\zeta)^\times$  as follows:

$$\begin{aligned} \mathcal{M}_5(M) &:= \{\gamma \in M(\zeta)^\times \mid \gamma^{-1+\tau} \notin M(\zeta)^5\}, \\ \mathcal{N}_5(M) &:= M(\zeta)^\times \setminus \mathcal{M}_5(M), \end{aligned}$$

where  $\tau$  is a generator of  $\text{Gal}(M(\zeta)/M)$ . Furthermore, we define a subset  $U(k)$  of  $\mathcal{O}_k$  as follows:

$$U(k) := \{\alpha \in \mathcal{O}_k \mid (N(\alpha), \text{Tr}(\alpha)) = 1, N(\alpha) \in \mathbb{Z}^5, \alpha \notin (\mathcal{O}_k)^5\}.$$

We consider the polynomial

$$\begin{aligned} f(X; \alpha) &:= f_5(X; \alpha) \\ &= X^5 - 5N(\alpha)X^3 + 5N(\alpha)^2X - N(\alpha)^2\text{Tr}(\alpha), \quad \alpha \in \mathcal{O}_k. \end{aligned}$$

Denote the minimal splitting field of  $f(X; \alpha)$  over  $\mathbb{Q}$  by  $K_\alpha$ .

First we show the following proposition.

**Proposition 4.1.** *Let the notation be as above. Then the following statements hold.*

(1) *For  $\alpha \in U(k)$ ,  $K_\alpha$  is normal over  $\mathbb{Q}$  and is a cyclic quintic extension of  $M$  unramified outside 5. Moreover, let  $\sigma$  and  $\iota$  be generators of  $\text{Gal}(K_\alpha/\mathbb{Q})$  with  $\sigma^5 = \iota^4 = 1$  and  $\iota|_M = \rho|_M$ . Then we have*

$$\text{Gal}(K_\alpha/\mathbb{Q}) = \langle \sigma, \iota \mid \sigma^5 = \iota^4 = 1, \iota^{-1}\sigma\iota = \sigma^{l(\rho)} \rangle.$$

(2) *Let  $E$  be an unramified cyclic quintic extension of  $M$ . Assume that  $E/\mathbb{Q}$  is normal and its Galois group is*

$$\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \iota \mid \sigma^5 = \iota^4 = 1, \iota^{-1}\sigma\iota = \sigma^{l(\rho)} \rangle \quad \text{with} \quad \iota|_M = \rho|_M.$$

*Then there exists an element  $\alpha \in U(k)$  so that we have  $E = K_\alpha$ .*

To prove this proposition, we need the following two lemmas.

**Lemma 4.2.** *The set  $U(k)$  is included in  $\mathcal{M}_5(M) \cap \mathcal{O}_k$ .*

*Proof.* Let  $\alpha$  be an element of  $U(k)$ . Since  $\alpha \notin (\mathcal{O}_k)^5$  and  $N(\alpha) \in \mathbb{Z}^5$ , we have  $\alpha^{-1+\tau} = \alpha^{-2}N(\alpha) \notin M(\zeta)^5$ . Therefore, we get  $\alpha \in \mathcal{M}_5(M) \cap \mathcal{O}_k$ .  $\square$

**Lemma 4.3.** (1) *For an element  $\alpha \in \mathcal{M}_5(M) \cap \mathcal{O}_k$ , we have  $K_\alpha = K_{\alpha^n}$  for every  $n \in \mathbb{Z}$ ,  $(n, 5) = 1$ .*

(2) *For two elements  $\alpha_1, \alpha_2 \in U(k)$ ,  $K_{\alpha_1} = K_{\alpha_2}$  if and only if  $\alpha_1^n = \alpha_2 x^5$  for some  $x \in k$  and  $n \in \{1, 2, 3, 4\}$ .*

*Proof.* (1) This result immediately follows from Proposition 3.2.

(2) For elements  $\alpha_1, \alpha_2 \in U(k)$ , we have

$$\begin{aligned} K_{\alpha_1} &= K_{\alpha_2} \\ \iff \alpha_1^n/\alpha_2 &\in \mathcal{N}_5(M) \text{ for some } n \in \{1, 2, 3, 4\} \quad (\text{by Proposition 3.2}) \\ \iff (\alpha_1^n/\alpha_2)^{-1+\tau} &\in M(\zeta)^5 \text{ for some } n \in \{1, 2, 3, 4\} \\ \iff (\alpha_1^n/\alpha_2)^{-2}N(\alpha_1^n/\alpha_2) &\in M(\zeta)^5 \text{ for some } n \in \{1, 2, 3, 4\} \\ \iff \alpha_1^n/\alpha_2 &\in M(\zeta)^5 \text{ for some } n \in \{1, 2, 3, 4\} \quad (\text{by } N(\alpha_1), N(\alpha_2) \in \mathbb{Z}^5) \\ \iff \alpha_1^n &= \alpha_2 x^5 \text{ for some } x \in M(\zeta) \text{ and } n \in \{1, 2, 3, 4\} \\ \iff \alpha_1^n &= \alpha_2 x^5 \text{ for some } x \in k \text{ and } n \in \{1, 2, 3, 4\} \quad (\text{by } 5 \nmid [M(\zeta) : k]). \end{aligned}$$

The proof is completed.  $\square$

*Proof of Proposition 4.1.* (1) Let  $\alpha$  be an element of  $U(k)$ . Then we have  $\alpha \in \mathcal{M}_5(M) \cap \mathcal{O}_k$  by Lemma 4.2. Hence by Proposition 3.1, we have only to show that  $K_\alpha/M$  is unramified outside 5. By applying Proposition 3.4 to  $f(X; \alpha)$ , we see that no primes except for 5 are totally ramified in  $\mathbb{Q}(\theta)$ , where  $\theta$  is a root of  $f(X; \alpha)$ . Then it follows from  $5 \nmid [M : \mathbb{Q}]$  that  $K_\alpha/M$  is unramified outside 5.

(2) Let  $E$  be an unramified cyclic quintic extension of  $M$ . Assume that  $E/\mathbb{Q}$  is normal and its Galois group is

$$\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \iota \mid \sigma^5 = \iota^4 = 1, \iota^{-1}\sigma\iota = \sigma^{\iota(\rho)} \rangle \quad \text{with} \quad \iota|_M = \rho|_M.$$

Then by Proposition 3.1 and Remark 3.3, there is an element  $\alpha \in \mathcal{M}_5(M) \cap \mathcal{O}_k$  so that we have  $E = K_\alpha$ .

Now let us show that we can take an element  $\beta \in U(k)$  with  $K_\alpha = K_\beta$ . We write  $\alpha = (a + b\sqrt{D})/2$ ,  $a, b \in \mathbb{Z}$ . Put  $g := (N(\alpha), \text{Tr}(\alpha))$ , and express

$$(4.1) \quad \begin{aligned} N(\alpha) &= gn, \\ \text{Tr}(\alpha) &= gt. \end{aligned}$$

Then we have  $n, t \in \mathbb{Z}$ ,  $(n, t) = 1$ , and

$$(4.2) \quad b^2D = g^2t^2 - 4gn.$$

Put  $g' := (g, n)$  and  $\beta := \alpha^2/gg'$ . Then we have  $K_\alpha = K_\beta$ . Indeed,  $K_\alpha = K_{\alpha^2}$  follows from Lemma 4.3 (1), and  $K_{\alpha^2} = K_\beta$  follows from  $f(X; \alpha^2) = g^5g'^5f(X/gg'; \beta)$ . Hence we have only to show  $\beta \in U(k)$ . By (4.1) and (4.2), we have

$$\begin{aligned} \beta &= \frac{(a + b\sqrt{D})^2}{4gg'} = \frac{a^2 + b^2D + 2ab\sqrt{D}}{4gg'} \\ &= \frac{g^2t^2 + (g^2t^2 - 4gn) + 2gtb\sqrt{D}}{4gg'} = \frac{gt^2 - 2n + tb\sqrt{D}}{2g'}. \end{aligned}$$

Since

$$N(\beta) = \frac{N(\alpha)^2}{g^2g'^2} = \frac{n^2}{g'^2} \in \mathbb{Z} \quad \text{and} \quad \text{Tr}(\beta) = \frac{gt^2 - 2n}{g'} \in \mathbb{Z},$$

we have  $\beta \in \mathcal{O}_k$ . Moreover we have

$$\left( \frac{n}{g'}, \frac{gt^2 - 2n}{g'} \right) = \left( \frac{n}{g'}, \frac{gt^2}{g'} \right) = 1,$$

so

$$(N(\beta), \text{Tr}(\beta)) = \left( \frac{n^2}{g'^2}, \frac{gt^2 - 2n}{g'} \right) = 1.$$

By the definition of  $\beta$ , we easily see  $\beta \in \mathcal{M}(M)$ . Hence we can apply Proposition 3.4 to  $f(X; \beta)$ . From the assumption that  $E/M$  is unramified, it must hold that  $v_q(N(\beta)) \equiv 0 \pmod{5}$  for every prime  $q$ . Then we have

$N(\beta) \in \mathbb{Z}^5$ . Finally, we show  $\beta \notin (\mathcal{O}_k)^5$ . Suppose, on the contrary, that  $\beta \in (\mathcal{O}_k)^5$ . Then there exist rational numbers  $u$  and  $v$  such that

$$\beta = \gamma^5 \quad \text{with} \quad \gamma = u + v\sqrt{D}.$$

Then because

$$\text{Tr}(\beta) = 2u(u^4 + 10u^2v^2D + 5v^4D^2) \quad \text{and} \quad N(\beta) = (u^2 - v^2D)^5,$$

we have

$$\begin{aligned} f(X; \beta) &= X^5 - 5(u^2 - v^2D)^5 X^3 \\ &\quad + 5(u^2 - v^2D)^{10} X - 2u(u^4 + 10u^2v^2D + 5v^4D^2)(u^2 - v^2D)^{10} \\ &= \{X - 2u(u^2 - v^2D)^2\} \{X^4 + 2u(u^2 - v^2D)^2 X^3 \\ &\quad - (u^2 - 5v^2D)(u^2 - v^2D)^4 X^2 - 2u(u^2 - 5v^2D)(u^2 - v^2D)^6 X \\ &\quad + (u^4 + 10u^2v^2D + 5v^4D^2)(u^2 - v^2D)^8\}. \end{aligned}$$

Hence  $f(X; \beta)$  is reducible over  $\mathbb{Q}$ . This contradicts  $K_\alpha = K_\beta$ . Hence we have  $\beta \notin (\mathcal{O}_k)^5$ . Therefore, we obtain  $\beta \in U(k)$ , as desired.  $\square$

Next we examine the ramification of the prime 5.

**Proposition 4.4.** *Let  $\alpha = (a + b\sqrt{D})/2$  ( $a, b \in \mathbb{Z}$ ) be an element of  $U(k)$  and let  $\theta$  be a root of  $f(X; \alpha)$ . Suppose that  $5 \mid b^2D$ . Then the following statements hold.*

- (1) *If  $v_5(b^2D) \geq 3$ , then the prime 5 is not totally ramified in  $\mathbb{Q}(\theta)/\mathbb{Q}$ .*
- (2) *If  $v_5(b^2D) = 1$  or 2, then the prime 5 is totally ramified in  $\mathbb{Q}(\theta)/\mathbb{Q}$ .*

*Proof.* Let  $\alpha = (a + b\sqrt{D})/2$  ( $a, b \in \mathbb{Z}$ ) be an element of  $U(k)$ , and suppose that  $5 \mid b^2D$ . Then neither  $N(\alpha)$  nor  $\text{Tr}(\alpha)$  is divisible by 5. Express  $N(\alpha) = m^5$ ,  $5 \nmid m \in \mathbb{Z}$ ; then we have

$$f(X; \alpha) = X^5 - 5m^5 X^3 + 5m^{10} X - m^{10} a.$$

This polynomial satisfies the condition (3.1) for  $j = 0$  because the constant term is not divisible by 5. Now let us apply Proposition 3.5 to  $f(X; \alpha)$ .

By  $5 \nmid a$  and  $5 \nmid m$ , we can verify that

$$v_5(a_0) = 0 \quad \text{and} \quad v_5(a_j) > 0 \quad \text{for every } j, \quad 1 \leq j \leq 3;$$

that is, the condition (S-i) does not hold, but the conditions both (S-ii-1) and (S-ii-2) hold.

We note that

$$\begin{aligned} f^{(1)}(X; \alpha) &= 5X^4 - 15m^5 X^2 + 5m^{10}, \\ f^{(2)}(X; \alpha) &= 20X^3 - 30m^5 X, \\ f^{(3)}(X; \alpha) &= 60X^2 - 30m^5. \end{aligned}$$

Then we have

$$\begin{aligned}
 f^{(1)}(m^{10}a; \alpha) &= 5(m^{10}a)^4 - 15m^5(m^{10}a)^2 + 5m^{10} \\
 &= 5m^{10}(m^{30}a^4 - 3m^{15}a^2 + 1) \\
 &= 5m^{10} \left\{ \left( \frac{a^2 - b^2D}{4} \right)^6 a^4 - 3 \left( \frac{a^2 - b^2D}{4} \right)^3 a^2 + 1 \right\} \\
 &= \frac{5m^{10}}{4^6} (a^{16} - 3 \cdot 4^3 a^8 + 4^6 + t_1 b^2 D)
 \end{aligned}$$

for some  $t_1 \in \mathbb{Z}$ . In a similar way, we get

$$\begin{aligned}
 f^{(2)}(m^{10}a; \alpha) &= 20(m^{10}a)^3 - 30m^5(m^{10}a) \\
 &= \frac{5m^{15}a}{16} (a^8 - 96 + t_2 b^2 D), \\
 f^{(3)}(m^{10}a; \alpha) &= 60(m^{10}a)^2 - 30m^5 \\
 &= \frac{15m^5}{16} (a^8 - 32 + t_3 b^2 D)
 \end{aligned}$$

for some  $t_2, t_3 \in \mathbb{Z}$ . Since the congruence equations  $a^{16} - 3 \cdot 4^3 a^8 + 4^6 \equiv 0 \pmod{5}$  and  $a^8 - 96 \equiv 0 \pmod{5}$  hold for all  $a \in \mathbb{Z}$  with  $(a, 5) = 1$ , and since  $X^8 - 32 = 0$  has no solution in  $\mathbb{Z}/5\mathbb{Z}$ , we have

$$(4.3) \quad v_5(f^{(3)}(m^{10}a; \alpha)) = 1$$

and

$$(4.4) \quad \frac{v_5(f^{(j)}(m^{10}a; \alpha))}{5-j} \geq \frac{1}{2} \quad \text{for every } j, 1 \leq j \leq 3.$$

It follows from the Eq. (4.3) that the condition (S-ii-4) holds for  $j = 3$ .

Now we have

$$\begin{aligned}
 f(m^{10}a; \alpha) &= (m^{10}a)^5 - 5m^5(m^{10}a)^3 + 5m^{10}m^{10}a - m^{10}a \\
 &= m^{10}a(m^{40}a^4 - 5m^{25}a^2 + 5m^{10} - 1) \\
 &= m^{10}a \left\{ \left( \frac{a^2 - b^2D}{4} \right)^8 a^4 - 5 \left( \frac{a^2 - b^2D}{4} \right)^5 a^2 + 5 \left( \frac{a^2 - b^2D}{4} \right)^2 - 1 \right\} \\
 &= \frac{m^{10}a}{4^8} (a^{20} - 5 \cdot 4^3 a^{12} + 5 \cdot 4^6 a^4 - 4^8 \\
 &\quad - 8a^{18}b^2D + 5^2 \cdot 4^3 a^{10}b^2D - 10 \cdot 4^6 a^2b^2D + t_4 b^4D^2)
 \end{aligned}$$

for some  $t_4 \in \mathbb{Z}$ . Here the congruence equation

$$a^{20} - 5 \cdot 4^3 a^{12} + 5 \cdot 4^6 a^4 - 4^8 \equiv 0 \pmod{5^3}$$

holds for all  $a \in \mathbb{Z}$  with  $(a, 5) = 1$ , because

$$\begin{aligned} X^{20} - 5 \cdot 4^3 X^{12} + 5 \cdot 4^6 X^4 - 4^8 \\ \equiv (X^4 - 1)(X^{16} + X^{12} - 69X^8 - 69X^4 + 36) \pmod{5^3}, \\ X^{16} + X^{12} - 69X^8 - 69X^4 + 36 \\ \equiv (X^4 - 1)^2(X^8 + 3X^4 + 11) \pmod{5^2} \end{aligned}$$

and  $a^4 - 1 \equiv 0 \pmod{5}$  for all  $a \in \mathbb{Z}$  with  $(a, 5) = 1$ . Hence we have

$$v_5(f(m^{10}a; \alpha)) \begin{cases} \geq 3 & \text{if } v_5(b^2D) \geq 3, \\ = v_5(b^2D) \leq 2 & \text{if } v_5(b^2D) = 1 \text{ or } 2. \end{cases}$$

From this together with the inequality (4.4), we see that the condition (S-ii-3) does not hold if  $v_5(b^2D) \geq 3$ , but holds if  $v_5(b^2D) = 1$  or  $2$ . This completes the proof of Proposition 4.4.  $\square$

## 5. PROOF OF THE MAIN THEOREM

The goal of this section is to prove our main theorem.

Let the notation be as in Sections 1 and 2. Moreover, put  $\alpha_{ir_i+1} := \varepsilon_i$ , if  $d > 0$ , and put

$$r'_i := \begin{cases} r_i + 1 & \text{if } d > 0, \\ r_i & \text{if } d < 0. \end{cases}$$

Define the set  $U(S(k_i))$  as follows:

$$U(S(k_i)) := \left\{ \prod_{j=1}^{r'_i} \alpha_{ij}^{t_{ij}} \mid 0 \leq t_{ij} \leq 4, \sum_{j=1}^{r'_i} t_{ij} \neq 0 \right\}.$$

The following proposition is important to prove our main theorem.

**Proposition 5.1.** *The family  $\{K_\alpha \mid \alpha \in U(S(k_i))\}$  of the minimal splitting fields  $K_\alpha$  of  $f(X; \alpha)$  over  $\mathbb{Q}$  for  $\alpha \in U(S(k_i))$  does not depend on the choice of generators of  $\text{Syl}_5^{\text{el}}\text{Cl}(k_i)$ .*

*Proof.* Let  $\text{Syl}_5^{\text{el}}\text{Cl}(k_i)$  be expressed as follows:

$$(5.1) \quad \text{Syl}_5^{\text{el}}\text{Cl}(k_i) = \langle [\mathfrak{b}_{i1}] \rangle \times \cdots \times \langle [\mathfrak{b}_{ir_i}] \rangle,$$

where  $\mathfrak{b}_{ij}$ ,  $1 \leq j \leq r_i$ , are (integral) ideals of  $k_i$ . Then  $\mathfrak{b}_{ij}^5$  is principal. Fix integer  $\beta_{ij} \in k_i$  with  $(\beta_{ij}) = \mathfrak{b}_{ij}^5$  for each  $j$ ,  $1 \leq j \leq r_i$ , and put  $\beta_{ir_i+1} := \varepsilon_i$ ,



if  $d > 0$ . Define the sets  $T(k_i)$  and  $U(T(k_i))$  by

$$T(k_i) := \{\beta_{ij} \mid 1 \leq j \leq r'_i\},$$

$$U(T(k_i)) := \left\{ \prod_{j=1}^{r'_i} \beta_{ij}^{t_{ij}} \mid 0 \leq t_{ij} \leq 4, \sum_{j=1}^{r'_i} t_{ij} \neq 0 \right\},$$

respectively. Moreover, put

$$\mathcal{A} := \{K_\alpha \mid \alpha \in U(S(k_i))\} \text{ and } \mathcal{B} := \{K_\beta \mid \beta \in U(T(k_i))\}.$$

To prove Proposition 5.1, it is sufficient to show that  $\mathcal{A} = \mathcal{B}$ .

Before proving this, we will show the following two lemmas.

**Lemma 5.2.** *Let the notation be as above. Then the following statements hold.*

- (1) *Let  $\beta$  be an element of  $U(T(k_i))$ . Assume that  $\beta$  is not divisible by any rational integers except  $\pm 1$ . Then  $\beta$  is also an element of  $U(k_i)$ .*
- (2) *For  $\alpha \in U(k_i)$ , there exists an element  $\beta \in U(T(k_i))$  so that we have  $K_\alpha = K_\beta$ .*

*Proof.* (1) Assume that  $\beta$  is an element of  $U(T(k_i))$  which is not divisible by any rational integers except  $\pm 1$ . It is easily seen that  $N(\beta) \in \mathbb{Z}^5$  and  $\beta \notin (\mathcal{O}_k)^5$ . Hence we have only to show  $(N(\beta), \text{Tr}(\beta)) = 1$ . Express  $\beta = (a + b\sqrt{D})/2$ ,  $a, b \in \mathbb{Z}$ , where  $D = d$  or  $5d$  according to  $i = 1$  or  $2$ , and express  $N(\beta) = m^5$ ,  $m \in \mathbb{Z}$ . Then we have

$$(5.2) \quad a^2 - b^2 D = 4m^5.$$

Assume that there exists a prime  $q$  so that we have  $q \mid (N(\beta), \text{Tr}(\beta))$ . Then by the Eq. (5.2), we have  $q^2 \mid b^2 D$ . Since  $D$  is square-free, we have  $q \mid b$ . Hence it follows from the assumption that  $q$  must be equal to 2. Put  $a = 2a'$ ,  $b = 2b'$ . Then we have  $a'^2 - b'^2 D = m^5$ . This implies

$$(5.3) \quad a'^2 - b'^2 D \equiv 0 \pmod{4},$$

and hence  $a' \equiv b' \pmod{2}$ . If  $a' \equiv b' \equiv 0 \pmod{2}$ , then we have  $2 \mid \beta$ . This is a contradiction. If  $a' \equiv b' \equiv 1 \pmod{2}$ , then we have  $D \equiv 1 \pmod{4}$  by the congruence equation (5.3). Therefore we have  $2 \mid \beta = a' + b'\sqrt{D}$ . This is a contradiction. Then we have  $(N(\beta), \text{Tr}(\beta)) = 1$ . Thus the assertion (1) of Lemma 5.2 has been proved.

(2) Let  $\alpha$  be an element of  $U(k_i)$ . First we show that  $\alpha$  is not divisible by any rational integers except  $\pm 1$ . Assume that the prime  $q$  divides  $\alpha$ . Then  $q$  also divides the conjugate of  $\alpha$ . We see, therefore, that  $q$  divides both  $N(\alpha)$  and  $\text{Tr}(\alpha)$ . This is a contradiction.

Now suppose that  $\alpha$  is a unit of  $k_i$ . Then we have  $\alpha = \pm \varepsilon_i^n$  for some  $n \in \mathbb{Z}$ ,  $(n, 5) = 1$ . Express  $n = 5n_1 + n_2$ ,  $n_1, n_2 \in \mathbb{Z}$ ,  $1 \leq n_2 \leq 4$ ; then we have  $\varepsilon_i^{n_2} = \beta_{i, r_i+1}^{n_2} \in U(T(k_i))$  and  $K_\alpha = K_{\varepsilon_i^{n_2}}$ .

Next suppose that  $\alpha$  is not a unit. Let  $\mathfrak{q}$  be a prime divisor of  $(\alpha)$  in  $k_i$ , and put  $q := \mathfrak{q} \cap \mathbb{Z}$ . Since  $\alpha$  is not divisible by any rational integers except  $\pm 1$  as we have seen,  $q$  is not inert in  $k_i$ . Assume that  $q$  is ramified in  $k_i$ ;  $(q) = \mathfrak{q}^2$ . Since  $q \mid N(\alpha)$  and  $N(\alpha) \in \mathbb{Z}^5$ , we have  $q^5 \mid N(\alpha)$ , and hence  $q \mid (\alpha)$ . This is a contradiction. Therefore all prime divisors of  $N(\alpha)$  split in  $k_i$ . Let

$$|N(\alpha)| = \prod_{l=1}^m q_l^{5e_l}$$

be the prime decomposition of  $|N(\alpha)|$  in  $\mathbb{Z}$ . For each  $q_l$ , express  $q_l = \mathfrak{q}_l \mathfrak{q}'_l$  in  $k_i$ . Choose the ideal  $\mathfrak{q}_l$  so that we have  $\mathfrak{q}_l \mid (\alpha)$  for each  $l$  ( $1 \leq l \leq m$ ); then we obtain

$$(\alpha) = \prod_{l=1}^m \mathfrak{q}_l^{5e_l} = \left( \prod_{l=1}^m \mathfrak{q}_l^{e_l} \right)^5.$$

Put  $\mathfrak{a} := \prod_{l=1}^m \mathfrak{q}_l^{e_l}$ . Since  $\alpha \notin (\mathcal{O}_{k_i})^5$ ,  $\mathfrak{a}$  is not principal. Then by (5.1) we can express

$$\mathfrak{a} = \mathfrak{b}_{i1}^{t_{i1}} \cdots \mathfrak{b}_{ir_i}^{t_{ir_i}}(\gamma), \quad 0 \leq t_{ij} \leq 4, \quad \sum_{j=1}^{r_i} t_{ij} \neq 0, \quad \gamma \in k_i.$$

Then we have

$$(\alpha) = (\beta_{i1}^{t_{i1}} \cdots \beta_{ir_i}^{t_{ir_i}} \gamma^5),$$

and hence

$$\alpha = \beta_{i1}^{t_{i1}} \cdots \beta_{ir'_i}^{t_{ir'_i}} \gamma'^5, \quad \gamma' \in k_i.$$

Then we have  $\beta := \beta_{i1}^{t_{i1}} \cdots \beta_{ir'_i}^{t_{ir'_i}} \in U(T(k_i))$  and  $K_\alpha = K_\beta$ . This completes the proof of Lemma 5.2.  $\square$

**Lemma 5.3.** *The number of distinct cyclic quintic extensions of  $M$  given as  $K_\alpha$  with  $\alpha \in U(T(k_i))$  is equal to  $(5^{r'_i} - 1)/4$ .*

*Proof.* For  $\beta, \beta' \in U(T(k_i))$ , we express

$$\beta = \beta_{i1}^{t_{i1}} \cdots \beta_{ir'_i}^{t_{ir'_i}}, \quad 0 \leq t_{ij} \leq 4,$$

$$\beta' = \beta_{i1}^{t'_{i1}} \cdots \beta_{ir'_i}^{t'_{ir'_i}}, \quad 0 \leq t'_{ij} \leq 4.$$

By using Lemma 4.3,  $K_\beta = K_{\beta'}$  if and only if there exists  $n \in \{1, 2, 3, 4\}$  such that we have  $nt_{ij} \equiv t'_{ij} \pmod{5}$  for all  $j$ ,  $1 \leq j \leq r'_i$ . Since  $\#U(T(k_i)) = 5^{r'_i} - 1$ , therefore, we obtain the desired conclusion.  $\square$

We go back to the proof of Proposition 5.1. Let  $\alpha$  be an element of  $U(S(k_i))$ . It follows from the choice of  $\mathfrak{a}_{ij}$  that  $\alpha$  is not divisible by any rational integers except  $\pm 1$ . Then by (1) of Lemma 5.2, we have  $\alpha \in U(k_i)$ . Hence by (2) of Lemma 5.2, we have on the one hand  $K_\alpha = K_\beta$  for some  $\beta \in U(T(k_i))$ . Therefore we have  $\mathcal{A} \subset \mathcal{B}$ . By Lemma 5.3, on the other hand, we have

$$\#\mathcal{A} = \#\mathcal{B} = \frac{5^{r'_i} - 1}{4}.$$

Hence we obtain  $\mathcal{A} = \mathcal{B}$ . The proof of Proposition 5.1 is completed.  $\square$

As we have seen in Section 2, we have only to study  $\text{Gal}(\overline{E}_i/M)$  ( $i = 1, 2$ ) for getting the 5-rank of  $\text{Cl}(M)$ , where  $\overline{E}_1$  (resp.  $\overline{E}_2$ ) is the composite field of all unramified cyclic quintic extensions of  $M$  of Type (I) (resp. of Type (II)). From now on, we calculate the 5-rank of  $\text{Gal}(\overline{E}_i/M)$ .

We recall that  $\rho$  is the fixed generator of  $\text{Gal}(M(\zeta)/k_1)$  with  $\zeta^\rho = \zeta^2$ . Assume that  $\alpha \in U(k_1)$  and take generators  $\sigma, \iota$  of  $\text{Gal}(K_\alpha/\mathbb{Q})$  with  $\sigma^5 = \iota^4 = 1$  and  $\iota|_M = \rho|_M$ . By applying Proposition 4.1 (1) to  $k = k_1$ , the relation  $\iota^{-1}\sigma\iota = \sigma^2$  holds. Hence if  $K_\alpha$  is unramified over  $M$ , then it is of Type (I). Next assume that  $\beta \in U(k_2)$ . Take generators  $\sigma, \iota$  of  $\text{Gal}(K_\beta/\mathbb{Q})$  with  $\sigma^5 = \iota^4 = 1$  and  $\iota|_M = \rho|_M$  and take a generator  $\rho'$  of  $\text{Gal}(M(\zeta)/k_2)$  with  $\iota|_M = \rho'|_M$ ; then we have  $\rho' = \tau\rho$ . Hence by Proposition 4.1 (1), we have

$$\iota^{-1}\sigma\iota = \sigma^{l(\rho')} = \sigma^{l(\tau\rho)} = \sigma^3$$

because  $\zeta^{\tau\rho} = (\zeta^{-1})^\rho = \zeta^{-2} = \zeta^3$ . If  $K_\beta/M$  is unramified, therefore,  $K_\beta$  is of Type (II).

From this, together with Proposition 4.1 (2), and Lemma 5.2, we have

**Proposition 5.4.** *For  $\alpha \in U(S(k_1))$  (resp.  $\beta \in U(S(k_2))$ ),  $K_\alpha$  is normal over  $\mathbb{Q}$  and is a cyclic quintic extension of  $M$  unramified outside 5. Moreover, if  $K_\alpha/M$  (resp.  $K_\beta/M$ ) is unramified, then  $K_\alpha$  (resp.  $K_\beta$ ) is of Type (I) (resp. of Type (II)). Conversely, suppose that  $E$  is an unramified cyclic quintic extension of  $M$ . If  $E$  is of Type (I) (resp. of Type (II)), then there exists an element  $\alpha \in U(S(k_1))$  (resp.  $\beta \in U(S(k_2))$ ) so that we have  $E = K_\alpha$  (resp.  $E = K_\beta$ ).*

By this proposition,  $\overline{E}_i$  coincides with the composite field of all unramified cyclic quintic extensions of  $M$  given as  $K_\alpha$  with  $\alpha \in U(S(k_i))$ .

The following proposition states a criterion for an element of  $U(S(k_i))$  to give an unramified extension of  $M$ .

**Proposition 5.5.** (1) For  $\alpha \in U(S(k_1))$ , we have

$K_\alpha/M$  is unramified

$$\iff \begin{cases} (\text{A-i}), (\text{A-ii}) \text{ or } (\text{A-iv}) & \text{if } d \equiv \pm 1 \pmod{5}, \\ (\text{A-i}), (\text{A-ii}), (\text{A-iii}) \text{ or } (\text{A-v}) & \text{if } d \equiv \pm 2 \pmod{5}. \end{cases}$$

(2) For  $\beta \in U(S(k_2))$ , we have

$$K_\beta/M \text{ is unramified} \iff (\text{B}).$$

*Proof.* (1) Let  $\alpha = (a + b\sqrt{d})/2$  ( $a, b \in \mathbb{Z}$ ) be an element of  $U(S(k_1))$ . It is clear by Proposition 5.4 that  $K_\alpha/M$  is unramified outside 5. Hence we have

$$K_\alpha/M \text{ is unramified} \iff \text{a prime divisor of 5 in } M \text{ is unramified in } K_\alpha.$$

Put

$$\alpha^l = \frac{a_l + b_l\sqrt{d}}{2}, \quad a_l, b_l \in \mathbb{Z},$$

for  $l (> 0) \in \mathbb{Z}$ .

First assume that  $d \equiv \pm 1 \pmod{5}$ . In this case, the prime 5 splits in  $k_1$ ;  $(5) = \mathfrak{p}\mathfrak{p}'$ . Then we have

$$(\mathcal{O}_{k_1}/(5))^\times = (\mathcal{O}_{k_1}/\mathfrak{p})^\times \times (\mathcal{O}_{k_1}/\mathfrak{p}')^\times \simeq C_4 \times C_4.$$

Since  $(\alpha, 5) = 1$ , therefore, we have  $\alpha^4 \equiv 1 \pmod{5}$ , and hence  $v_5(b_4) \geq 1$ . Since  $\alpha^4$  is not divisible by any rational integers except  $\pm 1$ , we can show  $\alpha^4 \in U(k_1)$  in the same way as the proof of Lemma 5.2 (1). It follows from Lemma 4.3 (1) that  $K_\alpha = K_{\alpha^4}$ . By applying Proposition 4.4 to  $f(X; \alpha^4)$ , therefore, we have

$$\begin{aligned} & \text{a prime divisor of 5 in } M \text{ is unramified in } K_\alpha \\ & \iff \text{a prime divisor of 5 in } M \text{ is unramified in } K_{\alpha^4} \\ & \iff 5 \text{ is not totally ramified in } \mathbb{Q}(\theta) \\ & \iff v_5(b_4) \geq 2, \end{aligned}$$

where  $\theta$  is a root of  $f(X; \alpha^4)$ . Here we note that

$$b_4 = \frac{ab(a^2 + b^2d)}{2}.$$

Moreover, an easy calculation shows that

$$\begin{aligned} v_5(a) \geq 2 & \iff (\text{A-ii}), \\ v_5(b) \geq 2 & \iff (\text{A-i}), \\ v_5(a^2 + b^2d) \geq 2 & \iff (\text{A-iv}). \end{aligned}$$

Hence by  $5 \nmid (a, b)$ ,  $5 \nmid (a, a^2 + b^2d)$  and  $5 \nmid (b, a^2 + b^2d)$ , we have

$$K_\alpha/M \text{ is unramified} \iff (\text{A-i}), (\text{A-ii}) \text{ or } (\text{A-iv}).$$

Next assume that  $d \equiv \pm 2 \pmod{5}$ . In this case, the prime 5 remains prime in  $k_1$ . In a similar way to the above argument, we have  $v_5(b_{24}) \geq 1$  because

$$(\mathcal{O}_{k_1}/(5))^\times \simeq C_{24}.$$

Moreover, we see that  $\alpha^{24} \in U(k_1)$  and  $K_\alpha = K_{\alpha^{24}}$ . By Proposition 4.4, therefore, we have

$$\begin{aligned} & \text{a prime divisor of 5 in } M \text{ is unramified in } K_\alpha \\ & \iff \text{a prime divisor of 5 in } M \text{ is unramified in } K_{\alpha^{24}} \\ & \iff 5 \text{ is not totally ramified in } \mathbb{Q}(\theta) \\ & \iff v_5(b_{24}) \geq 2, \end{aligned}$$

where  $\theta$  is a root of  $f(X; \alpha^{24})$ . Now we have

$$\begin{aligned} b_{24} &= \frac{1}{2^{20}} ab(3a^2 + b^2d)(a^2 + 3b^2d)(a^2 + b^2d)(a^4 + 14a^2b^2d + b^4d^2) \\ &\quad \times (a^4 + 6a^2b^2d + b^4d^2)(a^8 + 60a^6b^2d + 134a^4b^4d^2 + 60a^2b^6d^3 + b^8d^4). \end{aligned}$$

It is easily seen that

$$\begin{aligned} v_5(a) &\geq 2 \iff (\text{A-ii}), \\ v_5(b) &\geq 2 \iff (\text{A-i}), \\ v_5(3a^2 + b^2d) &\geq 2 \iff (\text{A-iii}), \\ v_5(a^2 + 3b^2d) &\geq 2 \iff (\text{A-v}), \end{aligned}$$

and the greatest common divisor of any pair of  $\{a, b, 3a^2 + b^2d, a^2 + 3b^2d\}$  is not divisible by 5. Furthermore,

$$\begin{aligned} & (a^2 + b^2d)(a^4 + 14a^2b^2d + b^4d^2)(a^4 + 6a^2b^2d + b^4d^2) \\ & \quad \times (a^8 + 60a^6b^2d + 134a^4b^4d^2 + 60a^2b^6d^3 + b^8d^4) = 0 \end{aligned}$$

has no solution in  $\mathbb{Z}/5\mathbb{Z}$  when  $5 \nmid (a, b)$  and  $d \equiv \pm 2 \pmod{5}$ . Hence the statement (1) of Proposition 5.5 has been proved.

(2) Let  $\beta = (a + b\sqrt{5d})/2$  ( $a, b \in \mathbb{Z}$ ) be an element of  $U(S(k_2)) \subset U(k_2)$ . Then by Proposition 4.4 and Proposition 5.4, we have

$$\begin{aligned} K_\beta/M \text{ is unramified} &\iff 5 \text{ is not totally ramified in } \mathbb{Q}(\theta) \\ &\iff v_5(b) \geq 1, \end{aligned}$$

where  $\theta$  is a root of  $f(X; \beta)$ . Since

$$v_5(b) \geq 1 \iff (\text{B}),$$

we obtain the desired conclusion.  $\square$

Now we define the integer  $\varphi$  by

$$\varphi := \begin{cases} 4 & \text{if } d \equiv \pm 1 \pmod{5}, \\ 24 & \text{if } d \equiv \pm 2 \pmod{5}. \end{cases}$$

For calculating the 5-rank of  $\text{Gal}(\overline{E}_1/M)$ , we need the following lemma.

**Lemma 5.6.** *Let  $\alpha, \alpha_1$  and  $\alpha_2$  be elements of  $U(S(k_1))$ .*

- (1) *If  $\alpha$  satisfies the condition (A-ii) (resp. (A-iii), (A-iv) or (A-v)), then  $\alpha^2$  (resp.  $\alpha^3, \alpha^4$  or  $\alpha^6$ ) satisfies (A-i).*
- (2) *If both  $\alpha_1$  and  $\alpha_2$  satisfy the condition (A-i), then so does the product  $\alpha_1\alpha_2$ .*
- (3) *If neither  $\alpha_1$  nor  $\alpha_2$  satisfies all of the five conditions (A-i) through (A-v), then one of the elements  $(\alpha_1\alpha_2)^\varphi, (\alpha_1^2\alpha_2)^\varphi, (\alpha_1^3\alpha_2)^\varphi$  and  $(\alpha_1^4\alpha_2)^\varphi$  satisfies the condition (A-i).*

*Proof.* Note that for  $\alpha = (a + b\sqrt{d})/2 \in U(S(k_1))$  ( $a, b \in \mathbb{Z}$ ), we have

$$(5.4) \quad (\text{A-i}) \iff v_5(b) \geq 2.$$

(1) By easy calculations, we give the results. Let us explain the case where  $\alpha = (s + t\sqrt{d})/2 \in U(S(k_1))$  ( $s, t \in \mathbb{Z}$ ) satisfies the condition (A-iii) for example. In this case, we have

$$s^2 \equiv \frac{s^2 - t^2d}{4} \pmod{5^2},$$

and hence  $3s^2 + t^2d \equiv 0 \pmod{5^2}$ . From this together with

$$\alpha^3 = \frac{s(s^2 + 3t^2d) + t(3s^2 + t^2d)\sqrt{d}}{8},$$

we see by (5.4) that  $\alpha^3$  satisfies (A-i).

(2) Assume that both elements  $\alpha_1 = (s + t\sqrt{d})/2$  ( $s, t \in \mathbb{Z}$ ) and  $\alpha_2 = (u + v\sqrt{d})/2$  ( $u, v \in \mathbb{Z}$ ) of  $U(S(k_1))$  satisfy the condition (A-i). Then by (5.4) we have  $v_5(t) \geq 2$  and  $v_5(v) \geq 2$ , and hence

$$(5.5) \quad v_5(sv + tu) \geq 2.$$

On the other hand, we have

$$\alpha_1\alpha_2 = \frac{su + tvd + (sv + tu)\sqrt{d}}{4}.$$

Then by (5.4) and (5.5), we conclude that  $\alpha_1\alpha_2$  satisfies (A-i).

(3) Let  $\alpha_1$  and  $\alpha_2$  be elements of  $U(S(k_1))$ . Assume that neither  $\alpha_1$  nor  $\alpha_2$  satisfies all of the five conditions (A-i) through (A-v). Then by Proposition 5.5 (1), a prime divisor of 5 in  $M$  is ramified in both  $K_{\alpha_1}$  and  $K_{\alpha_2}$ . Put

$$\alpha_1^\varphi = \frac{s + t\sqrt{d}}{2} \quad \text{and} \quad \alpha_2^\varphi = \frac{u + v\sqrt{d}}{2} \quad \text{with } s, t, u, v \in \mathbb{Z}.$$

Then both  $5 \mid t$  and  $5 \mid v$  hold as we have seen in the proof of (1) of Proposition 5.5. Since  $(\varphi, 5) = 1$ , we have  $K_{\alpha_1} = K_{\alpha_1^\varphi}$  and  $K_{\alpha_2} = K_{\alpha_2^\varphi}$ . Hence we have  $5^2 \nmid t$  and  $5^2 \nmid v$ . Write  $t = 5t'$  and  $v = 5v'$  ( $t', v' \in \mathbb{Z}$ ,  $5 \nmid t'v'$ ), and put

$$(\alpha_1^l \alpha_2)^\varphi = \frac{a_l + b_l \sqrt{d}}{2} \quad \text{with } a_l, b_l \in \mathbb{Z},$$

for  $l(>0) \in \mathbb{Z}$ . Then we have

$$\begin{aligned} b_1 &= \frac{5(sv' + t'u)}{2}, \\ b_2 &= \frac{5s(sv' + 2t'u) + 125t'^2 v'd}{4}, \\ b_3 &= \frac{5s^2(sv' + 3t'u) + 125t'^2(3sv' + t'u)d}{8}, \\ b_4 &= \frac{5s^3(sv' + 4t'u) + 250st'^2(3sv' + 2t'u)d + 3125t'^4 v'd^2}{16}. \end{aligned}$$

It is clear that one of those four elements is divisible by  $5^2$ . Hence by (5.4), we obtain the desired conclusion.  $\square$

We recall that the number of distinct cyclic quintic extensions of  $M$  given as  $K_\alpha$  with  $\alpha \in U(S(k_1))$  is equal to  $(5^{r'_1} - 1)/4$ .

Suppose that one of the five conditions (A-i) through (A-v) holds for every element of  $S(k_1)$ . Then by using Lemma 5.6 (1), we can choose  $u_j \in \{1, 2, 3, 4, 6\}$  so that  $\alpha_{1j}^{u_j}$  satisfies the condition (A-i) for each  $\alpha_{1j} \in S(k_1)$ . Put  $\alpha'_{1j} := \alpha_{1j}^{u_j}$ . Then we have

$$\text{Syl}_5^{\text{el}} \text{Cl}(k_1) = \langle [\mathbf{a}_{11}^{u_1}] \rangle \times \cdots \times \langle [\mathbf{a}_{1r'_1}^{u_{r'_1}}] \rangle,$$

and  $(\alpha'_{1j}) = (\mathbf{a}_{1j}^{u_j})^5$ . We define the set  $S'(k_1)$  by

$$S'(k_1) := \{\alpha'_{1j} \mid 1 \leq j \leq r'_1\},$$

and put

$$U(S'(k_1)) := \left\{ \prod_{j=1}^{r'_1} (\alpha'_{1j})^{t_{1j}} \mid 0 \leq t_{1j} \leq 4, \sum_{j=1}^{r'_1} t_{1j} \neq 0 \right\}.$$

It follows from (2) of Lemma 5.6 that all elements of  $U(S'(k_1))$  satisfy the condition (A-i). Then by Proposition 5.5 (1), all  $(5^{r'_1} - 1)/4$  fields given as  $K_\alpha$  with  $\alpha \in U(S'(k_1))$  are unramified over  $M$ . Therefore the 5-rank of  $\text{Gal}(\overline{E}_1/M)$  is equal to  $r'_1$ .

Next suppose that none of the five conditions (A-i) through (A-v) holds for some elements of  $S(k_1)$ .

First we consider the case where  $d > 0$  and the fundamental unit  $\varepsilon_1$  satisfies none of the five conditions (A-i) through (A-v). By Lemma 5.6 (3), there exists  $u_j \in \{0, 1, 2, 3, 4\}$  such that  $(\varepsilon_1^{u_j} \alpha_{1j})^\varphi$  satisfies (A-i) for each  $\alpha_{1j}$  ( $1 \leq j \leq r_1$ ). Put  $\alpha'_{1j} := \varepsilon_1^{u_j} \alpha_{1j}$ ; then we have

$$\text{Syl}_5^{\text{el}} \text{Cl}(k_1) = \langle [\mathbf{a}_{11}] \rangle \times \cdots \times \langle [\mathbf{a}_{1r_1}] \rangle,$$

and  $(\alpha'_{1j}) = (\mathbf{a}_{1j})^5$ . Put

$$S'(k_1) := \{\alpha'_{1j} \mid 1 \leq j \leq r_1\}$$

and

$$U(S'(k_1)) := \left\{ \prod_{j=1}^{r_1} (\alpha'_{1j})^{t_{1j}} \mid 0 \leq t_{1j} \leq 4, \sum_{j=1}^{r_1} t_{1j} \neq 0 \right\}.$$

It follows from (2) of Lemma 5.6 that all elements of  $U(S'(k_1))$  satisfy the condition (A-i). Then by Proposition 5.5 (1), all  $(5^{r_1} - 1)/4$  fields given as  $K_\alpha$  with  $\alpha \in U(S'(k_1))$  are unramified over  $M$ . However the number of unramified cyclic quintic extensions of  $M$  given as  $K_\alpha$  with  $\alpha \in U(S(k_1))$  is less than  $(5^{r_1+1} - 1)/4$ , because a prime divisor of 5 in  $M$  is ramified in  $K_{\varepsilon_1}$ ; that is,  $K_{\varepsilon_1}/M$  is not unramified. Therefore the 5-rank of  $\text{Gal}(\overline{E}_1/M)$  is equal to  $r_1 = r'_1 - 1$ .

Next we consider the case where “ $d < 0$ ” or “ $d > 0$  and the fundamental unit satisfies one of the five conditions (A-i) through (A-v).” We may assume that  $\alpha_{11}$  satisfies none of the five conditions (A-i) through (A-v). By Lemma 5.6 (3), for each  $\alpha_{1j}$  ( $2 \leq j \leq r_1$ ), there exists  $u_j \in \{0, 1, 2, 3, 4\}$  such that  $(\alpha_{11}^{u_j} \alpha_{1j})^\varphi$  satisfies the condition (A-i). Put  $\alpha'_{1j} := \alpha_{11}^{u_j} \alpha_{1j}$ ; then we have

$$\text{Syl}_5^{\text{el}} \text{Cl}(k_1) = \langle [\mathbf{a}_{11}] \rangle \times \langle [\mathbf{a}_{11}^{u_2} \mathbf{a}_{12}] \rangle \times \cdots \times \langle [\mathbf{a}_{11}^{u_{r_1}} \mathbf{a}_{1r_1}] \rangle$$

and  $(\alpha'_{1j}) = (\alpha_{11}^{u_j} \alpha_{1j})^5$ ,  $2 \leq j \leq r_1$ . When  $d > 0$ ,  $\varepsilon_1^u$  satisfies the condition (A-i) for some  $u \in \{1, 2, 3, 4, 6\}$ . Then we put  $\alpha'_{1r'_1} := \varepsilon_1^u$ . Put

$$S'(k_1) := \{\alpha'_{1j} \mid 2 \leq j \leq r'_1\}$$

and

$$U(S'(k_1)) := \left\{ \prod_{j=2}^{r'_1} (\alpha'_{1j})^{t_{1j}} \mid 0 \leq t_{1j} \leq 4, \sum_{j=2}^{r'_1} t_{1j} \neq 0 \right\}.$$



Then the number of unramified cyclic quintic extensions of  $M$  given as  $K_\alpha$  with  $\alpha \in U(S'(k_1))$  is equal to  $(5^{r'_1-1}-1)/4$ . Hence the 5-rank of  $\text{Gal}(\overline{E}_1/M)$  is equal to  $r'_1 - 1$ .

Next let us calculate the 5-rank of  $\text{Gal}(\overline{E}_2/M)$ . The following lemma corresponds to our Lemma 5.6.

**Lemma 5.7.** *Let  $\beta_1$  and  $\beta_2$  be elements of  $U(S(k_2))$ .*

- (1) *If both  $\beta_1$  and  $\beta_2$  satisfy the condition (B), then so does  $\beta_1\beta_2$ .*
- (2) *If neither  $\beta_1$  nor  $\beta_2$  satisfies the condition (B), then one of the elements  $\beta_1\beta_2$ ,  $\beta_1^2\beta_2$ ,  $\beta_1^3\beta_2$ ,  $\beta_1^4\beta_2$  satisfies the condition (B).*

*Proof.* We note that  $\beta = (a + b\sqrt{5d})/2 \in U(S(k_2))$  ( $a, b \in \mathbb{Z}$ ) satisfies the condition (B) if and only if  $v_5(b) \geq 1$ .

For  $\beta_1, \beta_2 \in U(S(k_2))$ , we express

$$\beta_1 = \frac{s + t\sqrt{5d}}{2} \quad \text{and} \quad \beta_2 = \frac{u + v\sqrt{5d}}{2} \quad \text{with } s, t, u, v \in \mathbb{Z}.$$

- (1) From the assumption, we have  $v_5(t) \geq 1$  and  $v_5(v) \geq 1$ . Since

$$\beta_1\beta_2 = \frac{su + 5tvd + (sv + tu)\sqrt{5d}}{4}$$

and  $v_5(sv + tu) \geq 1$ , we obtain the desired conclusion.

- (2) From the assumption, we have  $v_5(t) = 0$  and  $v_5(v) = 0$ . We also have  $v_5(s) = 0$  and  $v_5(u) = 0$  by  $(N(\beta_1), \text{Tr}(\beta_1)) = (N(\beta_2), \text{Tr}(\beta_2)) = 1$ . Put

$$\beta_1^l \beta_2 = \frac{a_l + b_l\sqrt{5d}}{2} \quad \text{with } a_l, b_l \in \mathbb{Z},$$

for  $l(>0) \in \mathbb{Z}$ . Then we have

$$\begin{aligned} b_1 &= \frac{sv + tu}{2}, \\ b_2 &= \frac{s(sv + 2tu) + 5t^2vd}{4}, \\ b_3 &= \frac{s^2(sv + 3tu) + 5t^2(3sv + tu)d}{8}, \\ b_4 &= \frac{s^3(sv + 4tu) + 10st^2(3sv + 2tu)d + 25t^4vd^2}{16}. \end{aligned}$$

It is clear that one of them is divisible by 5. The proof of Lemma 5.7 is completed.  $\square$

As in the above discussion, by using this lemma, we obtain that the 5-rank of  $\text{Gal}(\overline{E}_2/M)$  is equal to  $r'_2 - \delta_2$ .

We summarize the above argument in the following.

**Proposition 5.8.** *Let  $\overline{E}_1$  (resp.  $\overline{E}_2$ ) be the composite field of all unramified cyclic quintic extensions of  $M$  of Type (I) (resp. of Type (II)). Then we have*

$$\mathrm{Gal}(\overline{E}_i/M) \simeq \underbrace{C_5 \times \cdots \times C_5}_{r'_i - \delta_i} \quad (i = 1, 2),$$

where  $\delta_i$  is defined as in Section 1.

From this proposition together with the relation (2.2), we obtain that the 5-rank of the ideal class group of  $M$  is equal to  $r'_1 + r'_2 - \delta_1 - \delta_2$ . This completes the proof of the main theorem.

## 6. DIVISIBILITY OF THE CLASS NUMBERS

A necessary and sufficient condition for 3 to divide the class number of an imaginary quadratic field was given by Herz [3, Theorem 6]. In [8], Parry extended such a result to  $p = 5$ ; that is, he gave a necessary and sufficient condition for 5 to divide the class number of a certain imaginary cyclic quartic field. As an application of our main theorem, we can give another proof of Parry's result.

**Theorem 6.1** ([8, Theorem 2, Theorem 5, Corollary 6]). *Under the same situation as that in our main theorem, we assume in addition that  $d$  is positive. Let  $h_1$ ,  $h_2$  and  $h$  denote the class numbers of  $k_1$ ,  $k_2$  and  $M$ , respectively. Express  $\varepsilon_1 = (a_1 + b_1\sqrt{d})/2$  ( $a_1, b_1 \in \mathbb{Z}$ ) and  $\varepsilon_2 = (a_2 + b_2\sqrt{5d})/2$  ( $a_2, b_2 \in \mathbb{Z}$ ). Then  $5 \mid h$  if and only if one of the following conditions holds:*

- (P-i)  $a_1 \equiv 0 \pmod{5^2}$  or  $b_1 \equiv 0 \pmod{5^2}$ ;
- (P-ii)  $a_1 \equiv \pm 1, \pm 7 \pmod{5^2}$ ;
- (P-iii)  $b_2 \equiv 0 \pmod{5}$ ;
- (P-iv)  $5 \mid h_1 h_2$ .

*Proof.* Let  $r, r_1, r_2, \delta_1$  and  $\delta_2$  be the same notation as in our main theorem. Note that

$$\begin{aligned} \text{(P-i)} &\iff \mathrm{Tr}_{k_1}(\varepsilon_1) \equiv 0 \pmod{5^2} \text{ or } \mathrm{Tr}_{k_1}(\varepsilon_1)^2 \equiv 4N_{k_1}(\varepsilon_1) \pmod{5^3}, \\ \text{(P-ii)} &\iff \mathrm{Tr}_{k_1}(\varepsilon_1)^2 \equiv N_{k_1}(\varepsilon_1) \pmod{5^2}, \\ \text{(P-iii)} &\iff \mathrm{Tr}_{k_2}(\varepsilon_2)^2 \equiv 4N_{k_2}(\varepsilon_2) \pmod{5^2}. \end{aligned}$$

If the condition (P-iv) holds, then we have  $r_1 + r_2 \geq 1$ . If the condition (P-iv) does not hold, then we have  $S(k_i) = \{\varepsilon_i\}$  for  $i = 1, 2$ , and hence

$$\begin{aligned} \text{(P-i) or (P-ii)} &\implies \delta_1 = 0, \\ \text{(P-iii)} &\implies \delta_2 = 0. \end{aligned}$$

Therefore, if one of the above four conditions holds, then we have  $r = r_1 + r_2 + 2 - \delta_1 - \delta_2 \geq 1$ .

Conversely, assume that none of the above four conditions holds. Since both  $X^2 \equiv \pm 2 \pmod{5^2}$  and  $X^2 \equiv \pm 3 \pmod{5^2}$  have no solution in  $\mathbb{Z}$ ,  $\varepsilon_1$  does not satisfy either (A-iv) or (A-v). Then we have  $\delta_1 = \delta_2 = 1$  and  $r_1 + r_2 = 0$ . This implies  $r = 0$ ; that is,  $h$  is not divisible by 5.  $\square$

## 7. NUMERICAL EXAMPLES

In this section, we give some numerical examples.

**Example 7.1.** Let  $d = 2723$ . Then we have

$$\text{Cl}(k_1) \simeq C_2 \quad \text{and} \quad \text{Cl}(k_2) \simeq C_{20}.$$

Now we can write

$$\text{Syl}_5^{\text{el}} \text{Cl}(k_2) = \langle [\mathfrak{q}] \rangle,$$

where  $\mathfrak{q}$  is a prime divisor of 19 in  $k_2$  with  $(\beta) = \mathfrak{q}^5$ ,  $\beta = 1326 + 115\sqrt{5 \cdot 2723}$ . The fundamental unit  $\varepsilon_1 = 94137 + 1804\sqrt{2723}$  of  $k_1$  satisfies the condition (A-iii). Moreover both  $\beta$  and the fundamental unit  $\varepsilon_2 = 7001 + 60\sqrt{5 \cdot 2723}$  of  $k_2$  satisfy the condition (B). Then by the main theorem, the 5-rank  $r$  of  $M$  is equal to 3:

$$r = 0 + 1 + 2 - 0 - 0 = 3.$$

In fact, by using GP/PARI (version 2.1.0), we see that the ideal class group of  $M$  is isomorphic to  $C_{10} \times C_{10} \times C_{10} \times C_2$ .

**Example 7.2.** Let  $d = -14606$ . Then we have

$$\text{Cl}(k_1) \simeq C_{10} \times C_{10} \quad \text{and} \quad \text{Cl}(k_2) \simeq C_{44} \times C_2 \times C_2,$$

and we can write

$$\text{Syl}_5^{\text{el}} \text{Cl}(k_1) = \langle [\mathfrak{p}_1] \rangle \times \langle [\mathfrak{p}_2] \rangle,$$

where  $\mathfrak{p}_1$  and  $\mathfrak{p}_2$  are prime divisors of 71 and 73, respectively, in  $k_1$  with  $(\alpha_1) = \mathfrak{p}_1^5$ ,  $\alpha_1 = 39699 + 125\sqrt{-14606}$  and  $(\alpha_2) = \mathfrak{p}_2^5$ ,  $\alpha_2 = 19097 + 342\sqrt{-14606}$ . We can easily verify that  $\alpha_1$  and  $\alpha_2$  satisfy the conditions (A-i) and (A-iv), respectively. Then the main theorem follows that the 5-rank  $r$  of  $M$  is equal to 2:

$$r = 2 + 0 - 0 - 0 = 2.$$

In fact, by using GP/PARI (version 2.1.0), we see that the ideal class group of  $M$  is isomorphic to  $C_{10} \times C_{10} \times C_2$ .

**Example 7.3.** Let  $d = -16782$ . Then we have

$$\text{Cl}(k_1) \simeq C_{10} \times C_{10} \quad \text{and} \quad \text{Cl}(k_2) \simeq C_{40} \times C_2 \times C_2.$$

We can write

$$\mathrm{Syl}_5^{\mathrm{el}}\mathrm{Cl}(k_1) = \langle [\mathfrak{p}_1] \rangle \times \langle [\mathfrak{p}_2] \rangle \quad \text{and} \quad \mathrm{Syl}_5^{\mathrm{el}}\mathrm{Cl}(k_2) = \langle [\mathfrak{q}] \rangle,$$

where  $\mathfrak{p}_1$  and  $\mathfrak{p}_2$  are prime divisors of 7 and 31 in  $k_1$  respectively with  $(\alpha_j) = \mathfrak{p}_j^5$  ( $j = 1, 2$ ),  $\alpha_1 = 5 + \sqrt{-16782}$ ,  $\alpha_2 = 647 + 41\sqrt{-16782}$ , and  $\mathfrak{q}$  is a prime divisor of 271 in  $k_2$  with  $(\beta) = \mathfrak{q}^5$ ,  $\beta = 583699 + 3655\sqrt{-5 \cdot 16782}$ . We see that neither  $\alpha_1$  nor  $\alpha_2$  satisfy all of the five conditions (A-i) through (A-v), but  $(\alpha_1^3\alpha_2)^6$  satisfies (A-i) (cf. Lemma 5.6 (3)). Moreover, we also see that  $\beta$  satisfies the condition (B). Therefore it follows from the main theorem that the 5-rank  $r$  of  $M$  is equal to 2:

$$r = 2 + 1 - 1 - 0 = 2.$$

In fact, by using GP/PARI (version 2.1.0), we see that the ideal class group of  $M$  is isomorphic to  $C_{10} \times C_{10}$ .

**Example 7.4.** Let  $d = -560181$ . Then we have

$$\mathrm{Cl}(k_1) \simeq C_{334} \times C_2 \quad \text{and} \quad \mathrm{Cl}(k_2) \simeq C_{10} \times C_{10} \times C_{10}.$$

We note that  $k_2$  is the imaginary quadratic field with the largest discriminant which has ideal class group of 5-rank greater than two (see [1]). Now we have

$$\mathrm{Syl}_5^{\mathrm{el}}\mathrm{Cl}(k_2) = \langle [\mathfrak{q}_1] \rangle \times \langle [\mathfrak{q}_2] \rangle \times \langle [\mathfrak{q}_3] \rangle,$$

where  $\mathfrak{q}_1$ ,  $\mathfrak{q}_2$  and  $\mathfrak{q}_3$  are prime divisors of 181, 241 and 349, respectively, in  $k_2$  with  $(\beta_j) = \mathfrak{q}_j^5$  ( $j = 1, 2, 3$ ),

$$\begin{aligned} \beta_1 &= 426689 + 66\sqrt{-5 \cdot 560181}, \\ \beta_2 &= 91111 + 536\sqrt{-5 \cdot 560181}, \\ \beta_3 &= 2183773 + 382\sqrt{-5 \cdot 560181}. \end{aligned}$$

We can easily verify that none of  $\beta_j$  satisfies the condition (B). (Both  $\beta_1\beta_2$  and  $\beta_2\beta_3$  however satisfy (B).) Therefore, the main theorem follows that the 5-rank  $r$  of  $M$  is equal to 2:

$$r = 0 + 3 - 0 - 1 = 2.$$

In fact, by using GP/PARI (version 2.1.0), we see that the ideal class group of  $M$  is isomorphic to  $C_{10} \times C_{10}$ .

#### ACKNOWLEDGMENT

The author would like to thank the referee for his careful reading of the first version and for his comments which have improved the presentation of this paper.

## REFERENCES

- [1] D. A. BUELL, *Class groups of quadratic fields. II*, Math. Comp. **48**(1987) 85–93.
- [2] G. GRAS, *Théorèmes de réflexion*, J. Théor. Nombres Bordeaux **10**(1998) 399–499.
- [3] C. S. HERZ, *Construction of class fields*, in: “Seminar on Complex Multiplication,” Lecture Notes in Mathematics, Vol. **21**, Springer-Verlag, Berlin-New York, 1966.
- [4] M. IMAOKA AND Y. KISHI, *On dihedral extensions and Frobenius extensions*, in: “Galois Theory and Modular Forms,” pp. 195–220, Developments of Mathematics, Vol. **11**, Kluwer Acad. Publ., Dordrecht, 2003.
- [5] S.-N. KURODA, *Über den allgemeinen Spiegelungssatz für Galoissche Zahlkörper*, J. Number Theory **2**(1970) 282–297.
- [6] H.-W. LEOPOLDT, *Zur Struktur der  $l$ -Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199**(1958) 165–174.
- [7] D. J. MADDEN AND W. Y. VÉLEZ, *A note on the normality of unramified, abelian extensions of quadratic extensions*, Manuscripta Math. **30**(1979/80) 343–349.
- [8] C. J. PARRY, *Real quadratic fields with class numbers divisible by five*, Math. Comp. **32**(1978) 1261–1270.
- [9] M. SASE, *On a family of quadratic fields whose class numbers are divisible by five*, Proc. Japan Acad. Ser. A Math. Sci. **74**(1998) 120–123.
- [10] A. SCHOLZ, *Über die Beziehung der Klassenzahl quadratischer Körper zueinander*, J. Reine Angew. Math. **166**(1932) 201–203.
- [11] L. C. WASHINGTON, “Introduction to Cyclotomic Fields, 2nd ed.,” Graduate Texts in Mathematics, Vol. **83**, Springer-Verlag, New York, 1997.

YASUHIRO KISHI

DEPARTMENT OF MATHEMATICS  
 FUKUOKA UNIVERSITY OF EDUCATION  
 MUNAKATA, FUKUOKA 811-4192 JAPAN  
*e-mail address:* ykishi@fukuoka-edu.ac.jp

(Received June 30, 2004)