

On class number one problem in non-normal sextic CM-fields with imaginary quadratic subfields

Ryotaro OKAZAKI at Doshisha University

May 08 (Thursday) 2003

Abstract

Let K be a sextic CM-field which contains an imaginary quadratic subfield k . We give three necessary conditions for the relative class number of K to be one. The first condition (Theorem 1) is on ramification in k/\mathbf{Q} and K_+/\mathbf{Q} . The second condition (Theorem 2 complemented by Lemma 3) is on ramification in K/k and K_+/\mathbf{Q} . Let \mathfrak{l} be a prime ideal of K_+ whose inertia degree equals 1 or 2. Assume also \mathfrak{l} splits in K/K_+ . Then, the third condition (Theorem 6) estimates the norm of \mathfrak{l} from below by a constant determined by discriminants of k and K_+ .

1 Introduction

Let K be a CM-field, i.e., a totally imaginary quadratic extension of a totally real number field K_+ . The field K_+ is identified as the maximal totally real subfield of K . The ratio $h^-(K) = h(K)/h(K_+)$ of class numbers $h(K)$ and $h(K_+)$ of K and K_+ is called the relative class number of K . It is an integer by class field theory. Indeed, it is the order of the kernel of the norm map from the class group of K to that of K_+ .

We give three necessary conditions for a relative class number of a given sextic CM-field, which contains an imaginary quadratic subfield, to be one. In [13] and [15], we studied the case in which the sextic CM-field contains

no imaginary quadratic field. These necessary conditions are used in Bouteaux's challenge [1] for determination of sextic CM-fields of relative class number one. See [1] or [15] for related references.

We denote by $D(L)$ the absolute value of the discriminant of a given number field L . When K_+ is a totally real cubic field, the discriminant of the field $\mathbf{Q}(\sqrt{D(K_+)})$ is denoted by $D_0(K_+)$. Then, $f(K_+) = \sqrt{D(K_+)/D_0(K_+)}$ is a rational integer. (See [7].)

Two conditions are algebraic.

Theorem 1 *Let K be a sextic CM-field which contains an imaginary quadratic subfield k . Set $D = D(K_+)$. Assume $h^-(K)$ is odd. Then, we have*

- (i) *A unique prime number q is ramified in k/\mathbf{Q} ;*
- (ii) *A unique prime ideal \mathfrak{q} of K_+ is ramified in K/K_+ ;*
- (iii) *$q \in \mathfrak{q}$.*
- (iv) *The prime number q remains totally inertia in K_+/\mathbf{Q} if $q \nmid D$;*
- (v) *We have $D_0(K_+)/D(k) \equiv 3 \pmod{4}$ if $q = 2$ and $q \mid D_0(K_+)$.*

Theorem 2 *Let k and K be CM-fields such that $k \subset K$. Assume $p = [K : k]$ is an odd prime number. Denote by $t(K/k)$ [resp. $t(K_+/k_+)$] the number of prime ideals of k [resp. k_+] that are totally ramified in K/k [resp. K_+/k_+]. Set $R(K/k) = 0$ if K/k is generated by a p -th root of a unit of k , or K/k is not a radical extension. Otherwise set $R(K/k) = 1$. Then, we have*

$$p^{t(K/k)-t(K_+/k_+)-R(K/k)} h^-(k) \mid h^-(K).$$

In particular, the prime number p divides $h^-(K)$ if $R = 0$ and some prime ideal of k_+ ramifies totally in K_+/k_+ and at the same time splits in k/k_+ .

This generalizes Proposition 8 of [12] in which we assume K/k to be cyclic. In our situation, the exponent $R(K/k)$ in Theorem 2 is calculated by the following:

Lemma 3 *Let K be a CM-field which contains an imaginary quadratic field k . Then, K/k is a radical extension if and only if $k = \mathbf{Q}(\sqrt{-3D_0(K_+)})$. Moreover, K is generated by a cube root of a unit of k if and only if K equals the field K_9 generated over \mathbf{Q} by a primitive 9-th root of unity. In particular, $R(K/k) = 1$ if and only if $k = \mathbf{Q}(\sqrt{-3D_0(K_+)})$ and $K \neq K_9$.*

We need to introduce some notation before presenting the last condition.

Definition 4 When A, B, D, D_0 and f are positive real numbers, we define the quantity $\Delta = \Delta(A, B, c, D, D_0, f)$ by

$$\Delta(A, B, c, D, D_0, f) = \max \left\{ \frac{2f}{3}, (2D)^{1/3}, \sqrt{\frac{B^2 c D}{3A^2}} \right\}$$

and $C(A, B, c, D, D_0, f)$ by

$$C(A, B, c, D, D_0, f) = \begin{cases} \frac{1}{18}A^2f + \frac{1}{24}B^2cD_0f & \text{if } \frac{2f}{3} = \Delta; \\ \frac{1}{12}A^2(2D)^{1/3} + \frac{1}{36}B^2c \left(\frac{D^2}{2} \right)^{1/3} & \text{if } (2D)^{1/3} = \Delta; \\ \frac{1}{18}AB\sqrt{3cD} & \text{otherwise.} \end{cases}$$

We always have $C(A, B, c, D, D_0, f) \geq AB\sqrt{3cD}/18$.

Definition 5 Let K be a sextic CM-field which contains an imaginary quadratic subfield k . Assume that a unique prime number q is ramified in k/\mathbf{Q} and a unique prime ideal \mathfrak{q} of K_+ is ramified in K/K_+ . Put $d = D(k)$, $D = D(K_+)$, $D_0 = D_0(K_+)$ and $f = f(K_+)$. We define $C(K)$ by

$$C(K) = \begin{cases} C(q, 1, q, D, D_0, f) & \text{if } q \neq 2 \text{ and } q \nmid D; \\ C\left(1, 1, \frac{1}{q}, D, D_0, f\right) & \text{if } q \neq 2 \text{ and } q \mid D; \\ C(8, 4, 2, D, D_0, f) & \text{if } d = 8 \text{ and } 2 \nmid D; \\ C(4, 2, 2, D, D_0, f) & \text{if } d = 8 \text{ and } 2 \mid f; \\ C\left(1, 1, \frac{1}{2}, D, D_0, f\right) & \text{if } d = 8 \text{ and } 2 \mid D_0; \\ C(4, 4, 1, D, D_0, f) & \text{if } d = 4 \text{ and } 2 \nmid D; \\ C(1, 1, 1, D, D_0, f) & \text{if } d = 4 \text{ and } 2 \mid D. \end{cases}$$

We can now state the last condition:

Theorem 6 Let K be a sextic CM-field which contains an imaginary quadratic subfield k . Assume K_+ is a non-normal cubic field and $h^-(K) = 1$.

Let q be the prime number that is ramified in k/\mathbf{Q} . Put $d = D(k)$, $D = D(K_+)$, $D_0 = D_0(K_+)$ and $f = f(K_+)$.

Let l be a prime number. We have

$$l \geq C(K)$$

if

$$\left(\frac{-d}{l}\right) = 1, \quad \left(\frac{D}{l}\right) \neq 1.$$

We have

$$l \geq \sqrt{C(K)}$$

if

$$\left(\frac{-d}{l}\right) = -1, \quad \left(\frac{D}{l}\right) = -1.$$

We have

$$l \geq C(K)$$

if

$$l = q, \quad l \mid D_0, \quad l \nmid f, \quad \left(\frac{-D_0/d}{l}\right) = 1.$$

We also have

$$l \geq C(K)$$

if

$$\left(\frac{-d}{l}\right) = 1$$

and l splits completely in K_+/\mathbf{Q} .

Remark. The last assertion is also applicable to imaginary abelian sextic fields of relative class number one.

2 Algebraic Structure of Sextic CM-field

When L is a number field, we denote the ring of integers of L by $\mathfrak{O}(L)$.

Algebraic structure of a given cubic field is determined by the following:

Lemma 7 *Let K_+ be a totally real cubic field. Put $D_0 = D_0(K_+)$, $f = f(K_+)$ and $\mathfrak{o} = \mathfrak{O}(K_+)$. Let l be a prime number. Then, we have*

- (i) $l\mathfrak{o} = \mathfrak{l}^3$ for some prime ideal \mathfrak{l} of K_+ if $l \mid f$;
- (ii) $l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2^2$ for distinct prime ideals \mathfrak{l}_1 and \mathfrak{l}_2 of K_+ if $l \mid D_0$ and $l \nmid f$;
- (iii) $l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2$ for distinct prime ideals \mathfrak{l}_1 and \mathfrak{l}_2 of K_+ ($\deg \mathfrak{l}_1 = 1$ and $\mathfrak{l}_2 = 2$) if $(D_0/l) = -1$ and $l \nmid f$;
- (iv) l splits completely or remains totally in K/\mathbf{Q} if $(D_0/l) = +1$ and $l \nmid f$.
- (v) $l^3 \nmid f$
- (vi) $l^2 \nmid f$ if $l \neq 3$.
- (vii) $l \nmid \gcd(D_0, f)$ if $l \neq 3$;
- (viii) $K_+(\sqrt{D_0(K_+)})/\mathbf{Q}(\sqrt{D_0(K_+)})$ is a cyclic cubic extension.

See [7]. There, the statement is proved without assuming the cubic field to be totally real. Our restriction is simply for saving notation. **qed.**

The following Lemma will be used in our proof for Theorem 1.

Lemma 8 *Let k and K be CM-fields such that $k \subset K$. Assume $[K : k]$ is odd. Then, we have $h^-(k) \mid h^-(K)$.*

Proof. This is Corollary 29 of [14]. **qed.**

Proof of Theorem 1. By Lemma 8, the relative class number $h^-(k)$ divides the odd integer $h^-(K)$. Therefore, $h^-(k)$ is odd. By genus theory, this implies assertion (i).

Assertion (ii) is Lemma 6-(v) of [15].

Set $\mathfrak{o} = \mathfrak{D}(K_+)$

Assertion (iii) follows from Assertion (i) and (ii): indeed, $q\mathfrak{o}$ is not a square ideal since $[K_+ : \mathbf{Q}]$ is odd; on the other hand the ramification index, in K/\mathbf{Q} , of every prime ideal of K above q is even since ramification index of q in k/\mathbf{Q} is 2 by assertion (i); therefore, the ramification index, in K/K_+ , of some prime ideal of K_+ above q is 2; now assertion (ii) implies $q \in \mathfrak{q}$.

Assertion (iv) is Lemma 7 of [15].

Assume $q = 2$ and $q \mid D_0(K_+)$. Then, by Lemma 7-(ii) and (vii), the prime number 2 factors as

$$2\mathfrak{o} = \mathfrak{p}^2\mathfrak{p}'$$

in K_+ , where \mathfrak{p} and \mathfrak{p}' are distinct prime ideals of K_+ .

Let \mathfrak{P}' be a prime ideal of K above \mathfrak{p}' . Then, \mathfrak{P}' is ramified in K/\mathbf{Q} since 2 is ramified in k/\mathbf{Q} . On the other hand, \mathfrak{p}' is unramified in K_+/\mathbf{Q} . Therefore, the prime ideal \mathfrak{P}' must be ramified in K/K_+ . Thus, assertion (ii) implies $\mathfrak{p}' = \mathfrak{q}$.

Assertion (ii) also implies that \mathfrak{p} is not ramified in K/K_+ . The prime ideal \mathfrak{p} is not ramified in $K_+(\sqrt{D_0})/K_+$ since ramification index in the normal sextic extension $K_+(\sqrt{D_0})/\mathbf{Q}$ always divides 6. Therefore, \mathfrak{p} is not ramified in the normal quartic extension $K(\sqrt{D_0})/K_+$.

Therefore, the ramification index of 2 in the normal extension $K(\sqrt{D_0})/\mathbf{Q}$ equals 2. So does the the ramification index of 2 in $k(\sqrt{D_0})/\mathbf{Q}$. Recalling that 2 divides discriminants $-D(k)$ and $D_0 = D(\mathbf{Q}(\sqrt{D_0}))$, we now see 2 is not ramified in $\mathbf{Q}(\sqrt{-D_0/D(k)})/\mathbf{Q}$. Noting that $-D(k)$ is a prime discriminant, we then see $-D_0/D(k)$ is an integer congruent 1 modulo 4. We established assertion (v). **qed.**

Theorem 2 is a consequence of an analogous formula to the ambiguous class number formula [18, Sats 14 and 15]. Neither the ambiguous class number formula by itself nor its generalization (see [2, 10]) to normal extensions via cohomology is applicable in our situation since we are mainly dealing with the case in which K/k is non-normal. Therefore, we exploit an elementary method which was used in [8] and [16] for extensions over \mathbf{Q} and in [3] for relative extensions. This method has advantage over the genus theory [4, 5, 6] in that it captures contribution of all prime ideals that are ramified in extensions of our interest. Indeed, the limitation of genus theory, in investigation of divisors of class numbers, can be observed in its application [5, Theorem 5] to non-normal cubic fields. (See [9] for results of the elementary method and also for results of genus theory.) Let k and K be CM-fields such that $k \subset K$. Results in the literature give divisors of $h(K)/h(k)$ and $h(K_+)/h(k_+)$. On the other hand, we are interested in a divisor of $h^-(K)/h^-(k) = (h(K)/h(k))/(h(K_+)/h(k_+))$. Therefore, we prepare three Lemmata on radical extensions and CM-fields and carefully investigate the class groups of K and K_+ .

Lemma 9 *Let M/M_0 be an extension of number fields. Assume $p = [M : M_0]$ is a prime number. Let $\varepsilon \in M$ satisfy $\varepsilon^{p^n} = 1$ for some positive integer n . Then, we have $N_{M/M_0}\varepsilon = \varepsilon^p$. If $\varepsilon^p = 1$, then $\varepsilon \in M_0$.*

Proof. The second assertion follows after noting that $[M_0(\varepsilon) : M_0] < p = [M : M_0]$ and that M/M_0 is a primitive extension.

The first assertion is obvious if $\varepsilon \in M_0$. Assume $\varepsilon \notin M_0$. Then, ε^p is a primitive root p^m -th root of unity for some positive integer m by the second assertion. Thus, conjugates of ε over k are ε^{1+ip^m} ($i = 0, 1, \dots, p-1$). The first assertion is now obvious. **qed.**

When M is a number field, we denote the unit group of M by $E(M)$ and the group of roots of unity of M by $W(M)$.

Lemma 10 *Let k and K be CM-fields such that $k \subset K$. Assume $p = [K : k]$ is an odd prime number. Then, K_+/k_+ is not a radical extension.*

If K/k is generated by a p -th root of a unit of k , there exists an integer $m \geq 1$ and a primitive p^m -th root ζ of unity in k such that $K = k(\sqrt[p^m]{\zeta})$.

Proof. If K_+/k_+ is a radical extension, there is an element γ of K_+ such that $K_+ = k_+(\gamma)$ and $\gamma^p \in k_+$. Let ξ be a primitive p -th root of unity. Then, $\gamma\xi^i$ ($i = 0, 1, \dots, p-1$) are the conjugates of γ over k_+ . Since ξ is not totally real, this means K_+ is not totally real. By contradiction, we proved the first assertion.

Let $\varepsilon' \in E(K)$ be a generator of K/k such that $(\varepsilon')^p \in E(k)$. Set $\eta = N_{K/K_+}\varepsilon'$. Then, $\eta^p = N_{k/\mathbf{Q}}((\varepsilon')^p) \in E(k_+)$. By the first assertion, this implies $\eta \in E(k_+)$. The unit $(\varepsilon')^2/\eta$ also generates K/k . Here, we have $(\varepsilon')^2/\eta \in W(K)$ since $N_{K/K_+}((\varepsilon')^2/\eta) = 1$. Write the order of $(\varepsilon')^2/\eta$ as $p^{m'}n$ with integers m' and n such that $p \nmid n$. Then, by noting $((\varepsilon')^2/\eta)^p \in E(k)$, we see $\varepsilon = ((\varepsilon')^2/\eta)^n$ also generates K/k .

Set $\zeta = \varepsilon^p$. Then, by Lemma 9, we have $\zeta \neq 1$. Thus, the second assertion holds with $m' = m - 1$. **qed.**

When M/M_0 is an extension of number fields, the group $E(M/M_0)$ of relative units of M/M_0 is the group of units of M whose relative norm to M_0 equal 1. We define $V(M/M_0) = E(M)^{[M:M_0]}E(M_0) \cap E(M/M_0)$. When M is a CM-field, we denote by σ the complex conjugation of M .

Let k and K be CM-fields such that $k \subset K$. In the rest of this section, we use the following two identities of the norm-map: $N_{K/k}\gamma = N_{K_+/k_+}\gamma$ for $\gamma \in K_+$; $N_{K_+/k_+}N_{K/K_+}\Gamma = N_{K/k_+}\Gamma = N_{k/k_+}N_{K/k}\Gamma$ for $\Gamma \in K$. The former identity follows from $[K : k] = [K_+ : k_+]$. In particular, we have $N_{K/k}\gamma = 1$ if $\gamma \in K_+$ and $N_{K_+/k_+}\gamma = 1$; $N_{K_+/k_+}(N_{K/K_+}\Gamma) = 1$ if $\Gamma \in K$ and $N_{K/k}\Gamma = 1$.

Lemma 11 *Let k and K be CM-fields such that $k \subset K$. Assume $p = [K : k]$ is an odd prime number. Let ν and ι be the homomorphisms defined by*

$$\nu : \varepsilon \in E(K) \longmapsto N_{K/K_+}\varepsilon^{(p+1)/2} \in E(K_+)$$

and

$$\iota : \eta \in E(K_+) \longmapsto \eta \in E(K).$$

Then, ν and $\nu\iota$ induce respective identity maps on $E(K/k)/V(K/k)$ and $E(K_+/k_+)/V(K_+/k_+)$.

Proof. What we said before the Lemma implies that the map ι induces a homomorphism $E(K_+/k_+)/V(K_+/k_+) \longrightarrow E(K/k)/V(K/k)$ and that the map ν induces a homomorphism $E(K/k)/V(K/k) \longrightarrow E(K_+/k_+)/V(K_+/k_+)$.

We have $\nu\iota(\eta) = N_{K/K_+}\eta^{(p+1)/2} = \eta^{p+1} \in \eta V(K_+/k_+)$ for $\eta \in E(K_+/k_+)$. Therefore, $\nu\iota$ induces the identity map on $E(K_+/k_+)/V(K_+/k_+)$.

For studying ν , we show

$$W(K) \cap E(K/k) \subset V(K/k). \quad (1)$$

We decompose $W(K) \cap E(K/k)$ as $W(K) \cap E(K/k) = W'_p W_p$, where $p \nmid \#W'_p$ and $\#W_p$ is a power of p . We obviously have $W'_p = (W'_p)^p \subset E(K)^p \subset V(K/k)$. Inclusion (1) is now reduced to $W_p \cap E(K/k) \subset E(k) \cap E(K/k)$. Let ζ be a generator of $W_p \cap E(K/k)$. It suffice to show $\zeta \in E(k)$. By the first assertion of Lemma 9, we have $\zeta^p = N_{K/k}\zeta = 1$. Then, the second assertion of Lemma 9 implies $\zeta \in E(k)$, establishing (1).

Let $\varepsilon \in E(K/k)$. Then, we have $\varepsilon^{1-\sigma} \in W(K) \cap E(K/k) \subset V(K/k)$ by (1) and $\varepsilon^{1+\sigma} = N_{K/K_+}\varepsilon \in E(K_+/k_+)$. We now calculate $\nu\iota(\varepsilon) = (\varepsilon^{1+\sigma})^{(p+1)/2} = (\varepsilon^2/\varepsilon^{1-\sigma})^{(p+1)/2} = \varepsilon^{p+1}/(\varepsilon^{1-\sigma})^{(p+1)/2} \in \varepsilon V(K/k)$. Therefore, $\nu\iota$ induces the identity map on $E(K/k)/V(K/k)$. **qed.**

Proof of Theorem 2. The second assertion is an immediate consequence of the first assertion.

We discuss the case in which $R(K/k) = 0$. Indeed, we are more interested in this case. A way of treating the other case will be just remarked at the end of this proof.

Denote by $I(L)$ the group of ideals of a number field L and by $P(L)$ the group of principal ideals of L . Let $\phi_{K/k}$ be the lifting map $\mathfrak{b} \in I(k) \longmapsto \mathfrak{b}\mathfrak{D}(K) \in I(K)$ of ideals. Define $A(K) = \{\mathfrak{A} \in I(K) \mid \mathfrak{A}^p \in \phi_{K/k}I(k)\}$. Define the map ϕ_{K_+/k_+} and $A(K_+)$ in the same fashion. The assertion is then reduced to the claim

$$\frac{\#A(K)P(K)/P(K)}{\#A(K_+)P(K_+)/P(K_+)} \in p^{t(K/k)-t(K_+/k_+)-R(K/k)}h^-(k)\mathbf{Z}. \quad (2)$$

Indeed, this implies that the order $\#\ker(N_{K/K_+} : A(K)P(K)/P(K) \longrightarrow A(K_+)P(K_+)/P(K_+))$ is a multiple of $p^{t(K/k)-t(K_+/k_+)-R(K/k)}h^-(k)$. Since

this kernel is contained in $\ker(N_{K/K_+} : I(K)/P(K) \longrightarrow I(K_+)/P(K_+))$, the assertion will follow.

We evaluate $\#A(K)P(K)/P(K)$. We note that $\#A(K)/\phi_{K/k}I(k) = p^{t(K/k)}$ and hence $\#A(K)/\phi_{K/k}P(k) = p^{t(K/k)}h(k)$. Now, we calculate

$$\begin{aligned} \#A(K)P(K)/P(K) &= \#P(K)/(A(K) \cap P(K)) \\ &= \frac{\#A(K)/\phi_{K/k}P(k)}{\#(A(K) \cap P(K))/\phi_{K/k}P(k)} \\ &= \frac{p^{t(K/k)}h(k)}{\#(A(K) \cap P(K))/\phi_{K/k}P(k)}. \end{aligned} \quad (3)$$

For evaluating the denominator, we map $A(K) \cap P(K)/\phi_{K/k}P(k)$ in $E(K/k)/V(K/k)$. Consider the following process: for $\mathfrak{A} \in A(K) \cap P(K)$ choose a generator $\Gamma \in K$; then, $\Gamma^p/N_{K/k}\Gamma \in E(K/k)$. This defines a homomorphism $A(K) \cap P(K) \longrightarrow E(K/k)/V(K/k)$ since $\varepsilon^p/N_{K/k}\varepsilon \in V(K/k)$ for every $\varepsilon \in E(K)$. If $\mathfrak{A} \in \phi_{K/k}P(k)$ and $\Gamma \in k$ is a generator of \mathfrak{A} , we have $\Gamma^p/N_{K/k}\Gamma = 1$. Thus, our process defines the homomorphism

$$\phi_{K/k} : A(K) \cap P(K)/\phi_{K/k}P(k) \longrightarrow E(K/k)/V(K/k).$$

This homomorphism is injective as shown below. If \mathfrak{A} is a representative of a class in $\ker \psi_{K/k}$ and $\Gamma \in K$ is a generator of \mathfrak{A} , we have $\Gamma^p/N_{K/k}\Gamma = \varepsilon^p/\xi$ for some $\varepsilon \in E(K)$ and $\xi \in E(k)$. We then have $(\Gamma/\varepsilon)^p = (N_{K/k}\Gamma)/\xi \in k^\times$. Since we are discussing the case in which $R(K/k) = 0$, the extension K/k is not a radical extension or is generated by a p -th root ζ of some unit of k . If K/k is not a radical extension, the primitive extension K/k contains no non-trivial radical extension of k . Therefore, we get $\Gamma/\varepsilon \in k$ and hence $\mathfrak{A} \in \phi_{K/k}P(k)$. Otherwise, we can choose a suitable exponent i such that $\Gamma/\varepsilon\zeta^i \in k^\times$. Thus, we also get $\mathfrak{A} \in \phi_{K/k}P(k)$ in this case.

We can now rewrite (3) as

$$\#A(K)P(K)/P(K) = \frac{p^{t(K/k)}h(k)}{\#\text{Im } \psi_{K/k}}. \quad (4)$$

We can define ψ_{K_+/k_+} in the same fashion and prove

$$\#A(K_+)P(K_+)/P(K_+) = \frac{p^{t(K_+/k_+)}h(k_+)}{\#\text{Im } \psi_{K_+/k_+}} \quad (5)$$

by using Lemma 10.

Claim (2) is now reduced to

$$\mathrm{Im} \psi_{K/k} \simeq \mathrm{Im} \psi_{K_+/k_+}.$$

We use the maps ι and ν of Lemma 11. Then, this isomorphism is reduced to

$$\iota(\mathrm{Im} \psi_{K_+/k_+}) \subset \mathrm{Im} \psi_{K/k} \quad (6)$$

and

$$\nu(\mathrm{Im} \psi_{K/k}) \subset \mathrm{Im} \psi_{K_+/k_+}. \quad (7)$$

We show (6). Let $\eta \in E(K_+)$ be a representative of a class in $\mathrm{Im} \psi_{K_+/k_+}$. Without loss of generality, we assume existence of $\mathfrak{a} \in A(K_+) \cap P(K_+)$ and its generator $\gamma \in K_+$ such that $\eta = \gamma^p / N_{K_+/k_+} \gamma$. Then, we have $\iota(\eta) = \gamma^p / N_{K/k} \gamma$. Noting $\gamma \mathfrak{D}(K) \in A(K) \cap P(K)$, we now see $\iota(\eta V(K/k)) \in \mathrm{Im} \psi_{K/k}$.

We show (7). Let $\varepsilon \in E(K/k)$ be a representative of a class in $\mathrm{Im} \psi_{K/k}$. Without loss of generality, we assume existence of $\mathfrak{A} \in A(K) \cap P(K)$ and its generator $\Gamma \in K_+$ such that $\varepsilon = \Gamma^p / N_{K/k} \Gamma$. Put $\gamma = N_{K/K_+} \Gamma$. Then, we have $N_{K/K_+} N_{K/k} \Gamma = N_{k/k_+} N_{K/k} \Gamma = N_{K_+/k_+} N_{K/K_+} \Gamma = N_{K_+/k_+} \gamma$. Thus, $\nu(\varepsilon) = N_{K/K_+} (\Gamma^p / N_{K/k} \Gamma)^{(p+1)/2} = (\gamma^p / N_{K_+/k_+} \gamma)^{(p+1)/2}$. Noting that $\gamma \mathfrak{D}(K_+) \in A(K_+) \cap P(K_+)$, we now see $\nu(\varepsilon V(K/k)) \in \mathrm{Im} \psi_{K_+/k_+}$.

We established the first assertion in the case in which $R(K/k) = 0$.

The other case can be handled in the very similar way. The only differences are in (4), where we need to multiply the denominator by p , and in its proof, where we need to show $\ker \psi_{K/k} \simeq \mathbf{Z}/p\mathbf{Z}$. **qed.**

Proof of Lemma 3. Put $D_0 = D_0(K_+)$.

Assume K/k is a radical extension. Then, there is an element Γ of K^\times such that $\Gamma^3 \in k$ and $K = k(\Gamma)$. The extension $K(\sqrt{-3})/k(\sqrt{-3})$ is a Kummer extension. Since K and $\mathbf{Q}(\sqrt{-3})$ are CM-fields, the field $K(\sqrt{-3})$ is a CM-field. (See e.g. [14, Lemma 10].) Let F be the real quadratic field contained in $k(\sqrt{-3})$. Then, the sextic field K_+F is identified as the maximal totally real subfield of $K(\sqrt{-3})$. Hence, it will be a normal number field if $K(\sqrt{-3})$ is normal. This condition is verified as follows: we have $(N_{K/K_+} \Gamma)^3 = N_{K/K_+}(\Gamma^3) = N_{k/\mathbf{Q}}(\Gamma^3) \in \mathbf{Q}$; thus the first assertion of Lemma 10 implies $N_{K/K_+} \Gamma \in \mathbf{Q}$; the six conjugates of Γ over \mathbf{Q} are obtained by multiplying the three cube roots of unity to Γ and to $(N_{K/K_+} \Gamma)/\Gamma$; they all belong to $K(\sqrt{-3})$. Normality of K_+F now implies $F = \mathbf{Q}(\sqrt{D_0})$, i.e., $k = \mathbf{Q}(\sqrt{-3D_0})$.

We assume $k = \mathbf{Q}(\sqrt{-3D_0})$ for proving the converse. Let γ be a generator of K_+ whose trace to \mathbf{Q} equals 0. By solving the minimal polynomial of γ by Cardano formula, we see $\gamma = \alpha + \beta$, where $\alpha^3 \in k$ and $0 \neq \alpha\beta \in \mathbf{Q}$. Therefore, we get $K = k(\gamma) \subset k(\alpha)$. Since $[k(\alpha) : k] = 3 = [K : k]$, this implies $K = k(\alpha)$. We established the first assertion.

Assume K/k is generated by a cube root of a unit of k . Then, by Lemma 10, there exists an integer $m \geq 1$ and a primitive 3^m -th root ζ of unity in k such that $K = k(\sqrt[3]{\zeta})$.

Since k is a quadratic field, we must have $m = 1$ and $k = \mathbf{Q}(\zeta)$. The second assertion is now obvious.

The last assertion follows from the first two assertions. **qed.**

Remark. For further application of Cardano formula in quadratic and cubic fields, see [17] (application in class fields) or its refinement [11] (application in ring class fields).

3 Geometric Structure of Sextic CM-field

When α belongs to a totally real cubic field K_+ , we define $\|\alpha_\perp\|$ by

$$\|\alpha_\perp\| = \sqrt{\operatorname{tr}_{K_+/\mathbf{Q}} \left(\alpha - \frac{1}{3} \operatorname{tr}_{K_+/\mathbf{Q}} \alpha \right)^2}.$$

Then, we have $\operatorname{tr}_{K_+/\mathbf{Q}} \alpha^2 \geq \|\alpha_\perp\|^2$.

The following Lemma is used for studying geometry of sextic CM-fields.

Lemma 12 *Let $1, \alpha$ and β be integers of a totally real cubic field K_+ . Assume $\alpha \notin \mathbf{Q}$. Then, we have*

$$\|\alpha_\perp\| \geq \max \left\{ (2D)^{1/3}, \frac{2f}{3} \right\},$$

where $D = D(K_+)$ and $f = f(K_+)$. Assume $1, \alpha$ and β are linearly independent over \mathbf{Q} . Then, we have

$$\|\alpha_\perp\| \cdot \|\beta_\perp\| \geq \frac{D}{3}.$$

Proof. This is a part of Proposition 5 of [15].

qed.

Lemma 13 *Let K be a sextic CM-field which contains an imaginary quadratic subfield $k = \mathbf{Q}(\sqrt{-c})$, ($0 < c \in \mathbf{Q}$). Set $\mathfrak{o} = \mathfrak{D}(K_+)$. Let $\Lambda = (\alpha + \beta\sqrt{-c})/2$, ($\alpha, \beta \in \mathfrak{D}(K_+)$), be an integer of K such that $L = N_{K/K_+}\Lambda$ is a rational integer. Assume Λ does not belong to k nor K_+ . Assume also $\alpha \equiv a \pmod{A\mathfrak{o}}$ and $\beta \equiv b \pmod{B\mathfrak{o}}$ for some rational integers a, b, A and B such that $A^2 \geq cB^2$. Put $D = D(K_+)$, $D_0 = D_0(K_+)$ and $f = f(K_+)$. Then, we have*

$$L \geq C(A, B, c, D, D_0, f).$$

Proof. Write $\alpha = a + A\alpha'$ and $\beta = b + B\beta'$ with $\alpha', \beta' \in \mathfrak{D}(K_+)$. Then, we have

$$12L = \operatorname{tr}_{K_+/\mathbf{Q}} \alpha^2 + c \operatorname{tr}_{K_+/\mathbf{Q}} \beta^2 \geq \|\alpha_\perp\|^2 + c\|\beta_\perp\|^2 = A^2\|\alpha'_\perp\|^2 + cB^2\|\beta'_\perp\|^2.$$

Here, $1, \alpha'$ and β' are linearly independent over \mathbf{Q} . Otherwise, $1, \alpha$ and β are linearly dependent over \mathbf{Q} . Hence, we get quadratic equation of α or β over \mathbf{Q} by eliminating β or α from the equality $4L = \alpha^2 + c\beta^2$. Since K_+ is a cubic field, this implies α or β belongs to \mathbf{Q} . Hence, the equality $4L = \alpha^2 + c\beta^2$ implies β^2 or α^2 belongs to \mathbf{Q} according as $\alpha \in \mathbf{Q}$ or $\beta \in \mathbf{Q}$. Since K_+ is cubic, this implies the both of α and β belongs to \mathbf{Q} . This contradicts our assumption that Λ does not belong to k . (Note k is the unique quadratic subfield of K .)

We apply the second inequality of Lemma 12 to the previous inequality and obtain

$$12L \geq A^2\|\alpha'_\perp\|^2 + \frac{B^2cD}{3\|\alpha'_\perp\|^2}.$$

By using the inequality of arithmetic and geometric means and the first inequality of Lemma 12, we now establish the Lemma. **qed.**

Lemma 14 *Let K be a sextic CM-field which contains an imaginary quadratic field k . Assume that a unique prime number q is ramified in k/\mathbf{Q} and a unique prime ideal \mathfrak{q} of K_+ is ramified in K/K_+ . Let Λ be an integer of K such that $L = N_{K/K_+}\Lambda$ is a rational integer. Assume Λ does not belong to k nor K_+ . Put $d = D(k)$, $D = D(K_+)$, $D_0 = D_0(K_+)$ and $f = f(K_+)$. Then,*

we have

$$L \geq C(K) = \begin{cases} C(q, 1, q, D, D_0, f) & \text{if } q \neq 2 \text{ and } q \nmid D; & \text{(i)} \\ C\left(1, 1, \frac{1}{q}, D, D_0, f\right) & \text{if } q \neq 2 \text{ and } q \mid D; & \text{(ii)} \\ C(8, 4, 2, D, D_0, f) & \text{if } d = 8 \text{ and } 2 \nmid D; & \text{(iii)} \\ C(4, 2, 2, D, D_0, f) & \text{if } d = 8 \text{ and } 2 \mid f; & \text{(iv)} \\ C\left(1, 1, \frac{1}{2}, D, D_0, f\right) & \text{if } d = 8 \text{ and } 2 \mid D_0; & \text{(v)} \\ C(4, 4, 1, D, D_0, f) & \text{if } d = 4 \text{ and } 2 \nmid D; & \text{(vi)} \\ C(1, 1, 1, D, D_0, f) & \text{if } d = 4 \text{ and } 2 \mid D. & \text{(vii)} \end{cases}$$

Proof. We put $\mathfrak{o} = \mathfrak{D}(K_+)$.

Case (i): Since q is not ramified in K_+/\mathbf{Q} , the uniqueness of \mathfrak{q} implies that q remains inertia in K_+/\mathbf{Q} .

We can write $\Lambda = (\alpha + \beta\sqrt{-q})/2$ with $\alpha \in \mathfrak{o}$ and $\beta \in K_+$. Then, we have $4L = \alpha^2 + q\beta^2$. In particular, $q\beta^2 \in \mathfrak{o}$. Since q remains inertia in K_+/\mathbf{Q} , this implies $\beta \in \mathfrak{o}$.

We now have $4L \equiv \alpha^2 \pmod{q\mathfrak{o}}$. Since the residue field $\mathfrak{o}/q\mathfrak{o}$ is an extension of degree 3 of \mathbf{F}_q , this implies $\alpha \equiv a \pmod{q\mathfrak{o}}$ for some $a \in \mathbf{Z}$. Therefore, we can put $A = q$, $B = 1$ and $c = q$ in Lemma 13.

Case (ii): By Lemma 7-(i) and (ii), the prime number q decomposes as $q\mathfrak{o} = \mathfrak{p}^2\mathfrak{q}$ with prime ideals \mathfrak{p} and \mathfrak{q} of K_+ . (These primes \mathfrak{p} and \mathfrak{q} may or may not equal.)

We can write $\Lambda = (\alpha + \beta\sqrt{-q})/2$ with $\alpha \in \mathfrak{o}$ and $\beta \in K_+$. Then, we have $4L = \alpha^2 + q\beta^2$ and hence $q\beta^2 \in \mathfrak{o}$. In particular, $q\beta \in \mathfrak{o}$. Therefore, we can put $A = 1$, $B = 1$, $c = 1/q$ in Lemma 13.

Case (iii): As in case (i), the prime number $q = 2$ remains inertia in K_+/\mathbf{Q} .

We can write $\Lambda = (\alpha + \beta\sqrt{-2})/2$ with $\alpha \in \mathfrak{o}$ and $\beta \in K_+$. Then, we have $4L = \alpha^2 + 2\beta^2$. In particular, $2\beta^2 \in \mathfrak{o}$. Since 2 remains inertia in K_+/\mathbf{Q} , this implies $\beta \in \mathfrak{o}$. By repeating similar steps, we see $\alpha \in 2\mathfrak{o}$ and then $\beta \in 2\mathfrak{o}$. Write $\alpha = 2\alpha'$ and $\beta = 2\beta'$. Then, we have $L = (\alpha')^2 + 2(\beta')^2$.

Since the residue field $\mathfrak{o}/2\mathfrak{o}$ is an extension of degree 3 of \mathbf{F}_2 , any element of \mathfrak{o} satisfying quadratic congruence with coefficients in \mathbf{Z} modulo $2\mathfrak{o}$ is congruent to a rational integer modulo $2\mathfrak{o}$. We use this idea to show certain congruences of α and β . Firstly, $L \equiv (\alpha')^2 \pmod{2\mathfrak{o}}$ implies $\alpha' \equiv a' \pmod{2\mathfrak{o}}$.

(mod $2\mathfrak{o}$) for some $a' \in \mathbf{Z}$. Write $\alpha' = a' + 2\alpha''$. Then, $(L - (a')^2)/2 = 2a'\alpha'' + 2(\alpha'')^2 + (\beta')^2 \in \mathbf{Z}$. Secondly, $(L - (a')^2)/2 \equiv (\beta')^2 \pmod{2\mathfrak{D}}$ implies $\beta' \equiv b' \pmod{2\mathfrak{D}}$ for some $b' \in \mathbf{Z}$. Write $\beta' = b' + 2\beta''$. Then, we have $(L - (a')^2 - 2(b')^2)/4 = a'\alpha'' + (\alpha'')^2 + 2b'\beta'' + 2(\beta'')^2 \in \mathbf{Z}$. Lastly, $(L - (a')^2 - 2(b')^2)/4 \equiv a'\alpha'' + (\alpha'')^2 \pmod{2\mathfrak{o}}$ implies $\alpha'' \equiv a'' \pmod{2\mathfrak{o}}$ for some $a'' \in \mathbf{Z}$. We established $\alpha \equiv 2a' + 4a'' \pmod{8\mathfrak{o}}$ and $\beta \equiv 2b' \pmod{4\mathfrak{o}}$.

Therefore, we can put $A = 8$, $B = 4$ and $c = 2$ in Lemma 13.

Case (iv): By Lemma 7-(i), the prime number $q = 2$ ramifies totally as $q\mathfrak{o} = \mathfrak{q}^3$ in K_+/\mathbf{Q} .

We can write $\Lambda = (\alpha + \beta\sqrt{-2})/2$ with $\alpha \in \mathfrak{o}$ and $\beta \in K_+$. Then, we have $4L = \alpha^2 + 2\beta^2$. In particular, we have $2\beta^2 \in \mathfrak{o}$. Since $2\mathfrak{o} = \mathfrak{q}^3$, this implies $\beta \in \mathfrak{q}^{-1}$.

We can show $\alpha \in 2\mathfrak{o}$ and $\beta \in \mathfrak{q}^2$ as follows; suppose one of these conditions are broken; then the both of these conditions are broken; in other words, $\alpha^2, 2\beta^2 \notin \mathfrak{q}^6$; on the other hand, \mathfrak{q} divides α to an even order and $2\beta^2$ to an odd order; these contradicts the congruence $\alpha^2 + 2\beta^2 \equiv 0 \pmod{\mathfrak{q}^6}$.

We can write $\alpha = 2(a' + \alpha')$ with $a' \in \mathbf{Z}$ and $\alpha' \in \mathfrak{q}$ since $\alpha \in 2\mathfrak{o}$ and $\deg \mathfrak{q} = 1$. Thus, we have $L = (\alpha')^2 + \beta^2/2 = (a')^2 + 2a'\alpha' + (\alpha')^2 + \beta^2/2$. In particular, we have $L \equiv (a')^2 \pmod{\mathfrak{q}}$. Since $L, a' \in \mathbf{Z}$, this implies $L - (a')^2 \in 2\mathbf{Z}$. Therefore, $\beta^2/2 \equiv 0 \pmod{\mathfrak{q}^2}$. We now see $\beta \in 2\mathfrak{o}$.

We can write $\beta = 2(b' + \beta')$ with $b' \in \mathbf{Z}$ and $\beta' \in \mathfrak{q}$. Thus, we have $2a'\alpha' + (\alpha')^2 + 4b'\beta' + 2(\beta')^2 = L - (a')^2 - 2(b')^2 \in 2\mathbf{Z}$. In particular, $(\alpha')^2 \in \mathfrak{q}^3$ and hence $\alpha' \in \mathfrak{q}^2$. Hence, the left hand side belongs to \mathfrak{q}^4 . Since the right hand side is a rational integer, this implies $2a'\alpha' + (\alpha')^2 + 4b'\beta' + 2(\beta')^2 = L - (a')^2 - 2(b')^2 \in 4\mathbf{Z}$. In particular, we get $(\alpha')^2 \in \mathfrak{q}^5$. Thus, we see $\alpha' \in 2\mathfrak{o}$.

We have seen $\alpha \equiv 2a' \pmod{4\mathfrak{o}}$ and $\beta \equiv 0 \pmod{2\mathfrak{o}}$. Therefore, we can put $A = 4$, $B = 2$ and $c = 2$ in Lemma 13.

Case (v): This case is handled in exactly the same as case (ii).

Case (vi): As in case (i), the prime number $q = 2$ remains inertia in K_+/\mathbf{Q} .

We can write $\Lambda = (\alpha + \beta\sqrt{-1})/2$ with $\alpha \in \mathfrak{o}$ and $\beta \in K_+$. Then, we have $4L = \alpha^2 + \beta^2$. We get $\beta^2 = 4L - \alpha^2 \in \mathfrak{o}$ and hence $\beta \in \mathfrak{o}$.

We have $(\alpha - \beta)^2 = 4L - 2\alpha\beta$. Thus, we get $\alpha \equiv \beta \pmod{2\mathfrak{o}}$. Then, we see $2\alpha\beta = 4L - (\alpha - \beta)^2 \equiv 0 \pmod{4\mathfrak{o}}$. The two congruences imply $\alpha \equiv \beta \equiv 0 \pmod{2\mathfrak{o}}$.

Write $\alpha = 2\alpha'$ and $\beta = 2\beta'$. Then, we have $L = (\alpha')^2 + (\beta')^2$. Thus, $L = 2\alpha'\beta' + (\alpha' - \beta')^2 \equiv (\alpha' - \beta')^2 \pmod{2\mathfrak{o}}$. Since $\mathfrak{o}/2\mathfrak{o}$ is an extension of

degree 3 of \mathbf{F}_2 , this implies $\alpha' - \beta' \equiv a' \pmod{2\mathfrak{o}}$ for some $a' \in \mathbf{Z}$. Write $\alpha' = a' + \beta' + 2\gamma''$. Then, $L = (\alpha')^2 + (\beta')^2$ implies $a'\beta' + (\beta')^2 \equiv (L - (a')^2)/2 \pmod{2\mathfrak{o}}$. The consideration of the extension of finite fields again implies $\beta' \equiv b' \pmod{2\mathfrak{o}}$ for some $b' \in \mathbf{Z}$.

We have seen $\alpha \equiv 2(a' + b') \pmod{4\mathfrak{o}}$ and $\beta \equiv 2b' \pmod{4\mathfrak{o}}$. Therefore, we can put $A = 4$, $B = 4$ and $c = 1$ in Lemma 13.

Case (vii): By Lemma 7-(i) and (ii), the prime number q decomposes as $q\mathfrak{o} = \mathfrak{p}^2\mathfrak{q}$ with prime ideals \mathfrak{p} and \mathfrak{q} of K_+ . (These prime ideals \mathfrak{p} and \mathfrak{q} may or may not equal.)

We can write $\Lambda = (\alpha + \beta\sqrt{-1})/2$ with $\alpha \in \mathfrak{o}$ and $\beta \in K_+$. Then, we have $4L = \alpha^2 + \beta^2$ and hence $\beta^2 \in \mathfrak{o}$. In particular, $\beta \in \mathfrak{o}$. Therefore, we can put $A = 1$, $B = 1$, $c = 1$ in Lemma 13. **qed.**

4 Proof of Theorem 6

We begin with the following:

Lemma 15 *Let K be a CM-field. Assume $[K : \mathbf{Q}]/2$ and $h^-(K)$ are odd integers. Then, the group $E^+(K_+)$ of totally positive units of K_+ coincides with $E(K_+)^2$.*

Proof. This is assertion (ii) of Lemma 6 of [15]. **qed.**

Proof of Theorem 6. By Theorem 1, the field K satisfies the condition of Lemma 14 on the CM-field. Hence, our task is to construct the element Λ of $\mathfrak{D}(K)$.

We put $\mathfrak{o} = \mathfrak{D}(K_+)$.

We firstly discuss the case in which

$$\left(\frac{-d}{l}\right) = 1, \quad \left(\frac{D}{l}\right) = -1.$$

By Lemma 7-(iii), the prime number l decomposes in K_+ into a product of two prime ideals as $l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2$. On the other hand, the condition $(-d/l) = 1$ and the transfer theorem of class field theory imply \mathfrak{l}_1 and \mathfrak{l}_2 splits in K/K_+ . Let \mathfrak{L}_i and \mathfrak{L}'_i be the prime ideals of K above \mathfrak{l}_i ($i = 1, 2$).

Without loss of generality, we may assume $\mathfrak{L}_1\mathfrak{L}_2$ and $\mathfrak{L}'_1\mathfrak{L}'_2$ are lifted image of the two prime ideals of k above l . Since there are only two prime ideals of k above l , the product $\mathfrak{A} = \mathfrak{L}_1\mathfrak{L}'_2$ is not a lift of any ideal of k . Of course,

the splitting of \mathfrak{l}_1 and \mathfrak{l}_2 implies that \mathfrak{A} is not a lift of any ideal of K_+ . These two assertions imply that \mathfrak{A} is not generated by any element of k nor K_+ .

We have $l\mathfrak{o} = N_{K/K_+}(\mathfrak{A})$. Since $h^-(K) = 1$, this implies existence of a generator $\Gamma \in K$ of \mathfrak{A} . By Lemma 15, the totally positive unit $N_{K/K_+}\Gamma/l$ is a square of some unit ε of K_+ . By setting $\Lambda = \varepsilon^{-1}\Gamma$ and $L = l$ we get $L = N_{K/K_+}\Lambda$. As we have noted in the previous paragraph, Λ does not belong to k nor K_+ .

By applying Lemma 14, we see $l = L \geq C(K)$.

We secondly discuss the case in which

$$\left(\frac{-d}{l}\right) = 1, \quad \left(\frac{D}{l}\right) = 0.$$

By Lemma 7-(i) and (ii), the prime number L decomposes in K_+ as $l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2^2$, where \mathfrak{l}_1 and \mathfrak{l}_2 are prime ideals of K_+ . (The prime ideals \mathfrak{l}_1 and \mathfrak{l}_2 may or may not equal.) As in the first case, \mathfrak{l}_1 and \mathfrak{l}_2 splits in K/K_+ . Let \mathfrak{L}_i and \mathfrak{L}'_i be the prime ideals of K above \mathfrak{l}_i ($i = 1, 2$). We may assume $\mathfrak{L}_1\mathfrak{L}_2^2$ and $\mathfrak{L}'_1(\mathfrak{L}'_2)^2$ are lift of prime ideals of k above l .

Set $\mathfrak{A} = \mathfrak{L}_1(\mathfrak{L}'_2)^2$. Arguing in the same way as in the first case, we can find a generator Λ of \mathfrak{A} such that $l = N_{K/K_+}\Lambda$, $\Lambda \notin k$ and $\Lambda \notin K_+$. We set $L = l$. We repeat the same argument as in the first case to show $l \geq C(K)$.

We have now established the first assertion of the Theorem.

We thirdly discuss the case in which

$$\left(\frac{-d}{l}\right) = -1, \quad \left(\frac{D}{l}\right) = -1$$

and prove the second assertion of the Theorem. By Lemma 7-(iii), the prime number l decomposes in K_+ as $l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2$, where \mathfrak{l}_i is a prime ideal of degree i ($i = 1, 2$).

Since $N_{K_+/\mathbf{Q}}\mathfrak{l}_2 = l^2$ is a square, the transfer theorem of class field theory implies \mathfrak{l}_2 splits in K/K_+ . Let \mathfrak{L}_2 and \mathfrak{L}'_2 be the prime ideals of K above \mathfrak{l}_2 .

We set $\mathfrak{A} = \mathfrak{l}_1\mathfrak{L}'_2$. Obviously, this ideal is not a lift of any ideal of K_+ . It is not a lift of any ideal of k either. Otherwise, there is an ideal \mathfrak{a} of k such that $\mathfrak{a}\mathfrak{D}(K) = \mathfrak{A}$. By comparing norms, we see $N_{k/\mathbf{Q}}\mathfrak{a} = l^2$. Hence, \mathfrak{a} is a power of a prime ideal of degree 1 or equals $l\mathfrak{D}(k)$. In the former case, \mathfrak{a} and \mathfrak{a}^σ , where σ denotes the complex conjugation of K , are coprime. However, \mathfrak{A} and \mathfrak{A}^σ have the non-trivial common divisor \mathfrak{l}_1 , a contradiction. In the latter case, we must have $\mathfrak{a} = \mathfrak{a}^\sigma$, which contradicts $\mathfrak{A} \neq \mathfrak{A}^\sigma$.

We set $L = l^2$. By following the argument of the first case, we can find a generator Λ of \mathfrak{A} such that $L = N_{K/K_+}\Lambda$, $\Lambda \notin k$ and $\Lambda \notin K_+$.

By applying Lemma 14, we see $l^2 = L \geq C(K)$.

We nextly discuss the case in which

$$l = q, \quad l \mid D_0, \quad l \nmid f(K_+), \quad \left(\frac{-D_0/d}{l}\right) = 1.$$

By Lemma 7-(ii), the prime number l decomposes in K_+ as $l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2^2$, where \mathfrak{l}_1 and \mathfrak{l}_2 are distinct prime ideals.

Let $F = \mathbf{Q}(\sqrt{D_0})$, \mathfrak{P}_1 a prime ideal of FK_+ above \mathfrak{l}_1 and \mathfrak{P}_2 a prime ideal of FK_+ above \mathfrak{l}_2 . When M/M_0 is an extension of number fields and \mathfrak{P} is a prime ideal of M , we denote by $e(M/M_0, \mathfrak{P})$ the ramification index of \mathfrak{P} in M/M_0 . We have $2 \mid e(FK_+/\mathbf{Q}, \mathfrak{P}_2)$ since $e(K_+/\mathbf{Q}, \mathfrak{l}_2) = 2$. Normality of FK_+/\mathbf{Q} then implies $2 \mid e(FK_+/\mathbf{Q}, \mathfrak{P}_1)$. Since $e(K_+/\mathbf{Q}, \mathfrak{l}_1) = 1$, this implies $e(FK_+/\mathbf{Q}, \mathfrak{P}_1) = e(FK_+/K_+, \mathfrak{P}_1) = 2$. We further see $\deg \mathfrak{P}_1 = \deg \mathfrak{l}_1 = 1$.

Since FK_+/\mathbf{Q} is normal, we now see $e(FK_+/\mathbf{Q}, \mathfrak{P}_2) = 2$ and $\deg \mathfrak{P}_2 = 1$. Therefore, \mathfrak{l}_2 splits in FK_+/K_+ .

In our case, the prime number l splits in $\mathbf{Q}(\sqrt{-D_0/d})/\mathbf{Q}$. Thus, transfer theorem of class field theory implies splitting of \mathfrak{l} in $K_+(\sqrt{-D_0/d})/K_+$.

The results of the previous two paragraphs implies complete splitting of \mathfrak{l}_2 in the quartic extension $K_+(\sqrt{-D_0}, \sqrt{-D_0/d})/K_+$. Noting $k = \mathbf{Q}(\sqrt{-d})$ and $K = kK_+$, we now see \mathfrak{l}_2 splits in K/K_+ .

By Theorem 1-(iii), we then see \mathfrak{l}_1 is ramified in K/K_+ . Let \mathfrak{Q} be the prime ideal of K above \mathfrak{l}_1 and \mathfrak{L}_2 a prime ideal of K above \mathfrak{l}_2 . Put $\mathfrak{A} = \mathfrak{Q}\mathfrak{L}_2^2$. We repeat the same argument as in the second case to show $l = L \geq C(K)$, establishing the third assertion.

We lastly discuss the case in which

$$\left(\frac{-d}{l}\right) = 1$$

and l splits completely in K_+/\mathbf{Q} .

By the assumption, there are three different prime ideals $\mathfrak{l}_1, \mathfrak{l}_2$ and \mathfrak{l}_3 of K_+ such that $l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2\mathfrak{l}_3$.

By the transfer theorem of class field theory, the prime ideal \mathfrak{l}_i splits in K/K_+ , ($i = 1, 2, 3$). Let \mathfrak{L}_i and \mathfrak{L}'_i be the prime ideals of K above \mathfrak{l}_i .

We may assume $\mathfrak{L}_1\mathfrak{L}_2\mathfrak{L}_3$ and $\mathfrak{L}'_1\mathfrak{L}'_2\mathfrak{L}'_3$ are the lift of the two prime ideals of k above l .

We set $\mathfrak{A} = \mathfrak{L}_1\mathfrak{L}_2\mathfrak{L}'_3$ and $L = l$. We repeat the same argument as in the first case to show $l = L \geq C(K)$, establishing the last assertion. **qed.**

References

- [1] G. Bouteaux, “Le problème du nombre de classes 1 pour les corps à multiplication complexe sextiques non galoisiens”, preprint.
- [2] A. Brumer and M. Rosen, “Class number and ramification in number fields”, Nagoya Math. J. 23 (1963) 97–101.
- [3] I. Connell and D. Sussman, “The p -dimension of class groups of number fields”, J. London Math. Soc. (2) 2 (1970) 525–529.
- [4] A. Fröhlich, “The genus field and genus group in finite number fields”, Mathematika 6 (1959) 40–46.
- [5] —, “The genus field and genus group in finite number fields II”, Mathematika 6 (1959) 142–146.
- [6] Y. Furuta, “The genus field and genus number in algebraic number fields”, Nagoya Math. J. 29 (1967) 281–285.
- [7] H. Hasse, “Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage”, Math. Z. 31 (1930) 565–582; *Mathematische Abhandlungen Band 1*, de Gruyter, Berlin-New York (1975) 423–440.
- [8] M. Ishida, “A note on class numbers of algebraic number fields”, J. Number Theory 1 (1969) 65–69.
- [9] M. Ishida, *The genus fields of algebraic number fields*, LNM 555, Springer (1976).
- [10] K. Iwasawa, “A note on the group of units of an algebraic number field”, J. Math. Pures Appl. (9) 35 (1956), 189–192.
- [11] Y. Kishi, “A constructive approach to Spiegelung relations between 3-ranks of absolute ideal class groups and congruent ones modulo $(3)^2$ in quadratic fields”, J. Number Theory 83 (2000) 1–49.

- [12] S. Louboutin, R. Okazaki and M. Olivier, “The class number one problem for some non-abelian normal CM-fields”, *Trans. A.M.S.* 349 (1997) 3567–3678.
- [13] R. Okazaki “Non-normal class number one problem and the least prime power-residue”, in *Number Theory and its Applications* (S. Kanemitsu and K. Györy eds.) Kluwer Academic Publishers (1999) 273–289.
- [14] R. Okazaki, “Inclusion of CM-fields and divisibility of relative class numbers”, *Acta Arith.* 92 (2000) 319–338.
- [15] —, “On class number one problem in non-normal sextic CM-fields”, *preprint*.
- [16] P. Roquette and H. Zassenhaus, “A class of rank estimate for algebraic number fields”, *J. London Math. Soc.* 44 (1969) 31–38.
- [17] A. Scholz, “Über die Beziehung der Klassenzahlen quadratischer Körper zueinander”, *J. reine angew. Math.* 166 (1932) 201–203.
- [18] T. Takagi, “Über eine Theorie des relativ Abel’schen Zahlkörpers”, *J. College Sci. Imperial Univ. Tokyo* 41 (1920) 1–33; *Teiji Takagi Collected papers*, Springer (1990) 73–167.

Ryotaro OKAZAKI,
 Doshisha University,
 Department of Mathematics,
 Kyotanabe, Kyoto, 610-0394, JAPAN
 email: rokazaki@dd.ij4u.or.jp
<http://www1.doshisha.ac.jp/~rokazaki>