

# On class number one problem in non-normal sextic CM-fields

Ryotaro OKAZAKI at Doshisha University

May 08 (Thursday) 2003

## Abstract

Let  $K$  be a sextic CM-field field which contains no imaginary quadratic subfield. We give a necessary condition for the relative class number of  $K$  to be one. Let  $\mathfrak{l}$  be a prime ideal of  $K_+$  which splits in  $K/K_+$ . Then, Theorem 3 estimates the norm of  $\mathfrak{l}$  from below by a constant determined by the discriminants of  $K$  and  $K_+$ . It is used for proving our necessary condition (Theorem 2), which estimates prime numbers satisfying certain conditions written in terms of the Kronecker symbol and the mentioned discriminants. A necessary and sufficient condition, in terms of ramification, for a given sextic CM-field of odd relative class number to contain an imaginary quadratic field is also given in Lemma 7.

## 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 will give a necessary condition for the relative class number of a given sextic CM-fields  $K$ , containing no imaginary quadratic subfield, to be one. Let  $K$  be a sextic CM-field. Our main concern in this paper is the case in which  $K_+$  is non-normal and  $K$  contains no imaginary quadratic subfield. In

[11], we have already studied the case in which  $K_+$  is normal and  $K$  contains no imaginary quadratic subfield. In [13], we study the case in which  $K$  contains an imaginary quadratic subfield. The necessary conditions in this series of studies are used in Boutteaux's challenge [2] of determination of sextic CM-fields of class number one. This is a big step after determination of imaginary abelian sextic CM-fields of relative class number one by Kwon-Park [8], Uchida [17] and Yamamura [19]; and after determination of non-normal quartic CM-fields of relative class number one by Louboutin-Okazaki [10]. Note that imaginary abelian fields of relative class number one are determined by Chang-Kwon [3] and Yamamura [19]. Recent progress in determination of normal CM-fields of (relative) class number one is found in Chang-Kwon [4] and its references. A recent study of analytic part of the problem is found in Bessasi [1].

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].)

The condition is written in terms of the following quantity:

**Definition 1** *Let  $K$  be a sextic CM-field. Put  $D = D(K_+)$ ,  $d = d(K) = D(K)/D^2$ ,  $D_0 = D_0(K_+)$  and  $f = f(K_+)$ . Define the function  $C(x, y)$  of positive real numbers  $x$  and  $y$  by*

$$C(x, y) = \frac{1}{12} \left( 2^{1/3} x^{1/3} + \sqrt{\frac{1}{2^{4/3}} x^{2/3} + 9y^{2/3}} \right)$$

and the function  $C'(D, y)$  by

$$C'(D, y) = \begin{cases} \frac{1}{12} \left( \frac{2}{3} f + \sqrt{\frac{3}{4} D_0 f + 9y^{2/3}} \right) & \text{if } \frac{2}{3} f \geq \sqrt[3]{2D}; \\ C(D, y) & \text{otherwise.} \end{cases}$$

Our main assertion is the following:

**Theorem 2** *Let  $K$  be a sextic CM-field. Assume  $K_+$  is a non-normal cubic field and  $K$  contains no imaginary quadratic subfield. Let  $D = D(K_+)$  and  $d = d(K)$ . Assume also  $h^-(K) = 1$ . Then, a unique prime ideal  $\mathfrak{q} = \mathfrak{q}(K)$  is ramified in  $K/K_+$ . Let  $q'$  be the prime number contained in  $\mathfrak{q}$  if  $\deg \mathfrak{q}$  is*

odd or  $-4$  if  $\deg \mathfrak{q}$  is even. (Then,  $d/q'$  is a square in  $\mathbf{Z}$ .) Let  $l$  be a prime number. If

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

we have

$$l > C' \left(D, \frac{d^2}{2^6}\right)^{1/2}, \quad \frac{d^{1/2}}{2^3}.$$

If

$$\left(\frac{-q'}{l}\right) = +1 \quad \& \quad \left(\frac{D}{l}\right) = 0.$$

we have

$$l > C' \left(D, \frac{d^3}{2^{12}}\right), \quad \frac{d}{2^6}.$$

If

$$\left(\frac{-q'}{l}\right) = +1 \quad \& \quad \left(\frac{D}{l}\right) = +1,$$

we have

$$l > C' \left(D, \frac{d^2}{2^6}\right)^{1/2}$$

and we also have either

$$l > C \left(D, \frac{d^3}{2^{12}}\right)^{3/4}, \quad \frac{d}{2^6}$$

or

$$l > C' (D, d), \quad \frac{d^{1/3}}{2^2}.$$

In particular,

$$\left(\frac{-q'}{l}\right) \left(\frac{D}{l}\right) = +1$$

implies

$$l > C' \left(D, \frac{d^2}{2^6}\right)^{1/2}.$$

**Remark.** Here, the symbol  $(\bullet/\bullet)$  is the Kronecker symbol and we regard  $(\pm 2/\bullet) = (\pm 8/\bullet)$ .

We can state stronger conditions if we use the arithmetic of  $K$ . Indeed, Theorem 2 is a consequence of the following:

**Theorem 3** *Let  $K$  be a sextic CM-field which contains no imaginary quadratic subfield. Assume also  $h^-(K) = 1$ . Put  $\mathfrak{o} = \mathfrak{D}(K_+)$ ,  $D = D(K_+)$  and  $d = d(K)$ . Let  $\mathfrak{l}$  be a prime ideal of  $K_+$  which splits in  $K/K_+$  and  $l$  the prime number in  $\mathfrak{l}$ . Then, we have*

$$l \geq \left( \frac{d}{64} \right)^{1/\deg \mathfrak{l}}.$$

*We have estimates of  $l$  depending on decomposition of  $l$  in  $K_+$ :*

$$\begin{array}{llll} l > C'(D, d) & \text{if } \mathfrak{l}\mathfrak{o} = \mathfrak{l}_1 & \text{and } \mathfrak{l} = \mathfrak{l}_1; \\ l > C'(D, d^3/2^{12}) & \text{if } \mathfrak{l}\mathfrak{o} = \mathfrak{l}_1^3, & \text{and } \mathfrak{l} = \mathfrak{l}_1; \\ l > C'(D, d^3/2^{12}) & \text{if } \mathfrak{l}\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2^2, \quad \mathfrak{l}_1 \neq \mathfrak{l}_2 & \text{and } \mathfrak{l} = \mathfrak{l}_1; \\ l^2 > C'(D, d^5/2^{24}) & \text{if } \mathfrak{l}\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2^2, \quad \mathfrak{l}_1 \neq \mathfrak{l}_2 & \text{and } \mathfrak{l} = \mathfrak{l}_2; \\ l^2 > C'(D, d^5/2^{24}) & \text{and} \\ l^{4/3} > C(D, d^3/2^{12}) & \text{if } \mathfrak{l}\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2, \quad \deg \mathfrak{l}_2 = 2 & \text{and } \mathfrak{l} = \mathfrak{l}_1; \\ l^2 > C'(D, d^2/2^6) & \text{if } \mathfrak{l}\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2, \quad \deg \mathfrak{l}_2 = 2 & \text{and } \mathfrak{l} = \mathfrak{l}_2; \\ l^2 > C'(D, d^5/2^{24}) & \text{and} \\ l^{4/3} > C(D, d^3/2^{12}) & \text{if } \mathfrak{l}\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2\mathfrak{l}_3, \quad \mathfrak{l}_1 \neq \mathfrak{l}_2 \neq \mathfrak{l}_3 \neq \mathfrak{l}_1 & \text{and } \mathfrak{l} = \mathfrak{l}_1. \end{array}$$

*The expression  $C(D, *)$  [resp.  $C'(D, *)$ ] in the right hand side of this list can be replaced with  $C(D, d)$  [resp.  $C'(D, d)$ ].*

*In particular, we have*

$$l > \sqrt{C'(D, d^2/2^6)}.$$

*If  $l = q(K)$  and  $l$  does not split completely in  $K_+/\mathbf{Q}$ , we have*

$$l > C'(D, d).$$

*If every prime ideal of  $K_+$  above  $l$  splits in  $K/K_+$ , we also have*

$$l > C'(D, d).$$

**Remark.** When  $K_+$  is a cyclic cubic field, the first and the last cases of the second assertion slightly improve upon Theorem 2 of [11].

The key to the Theorems is the following estimate:

**Lemma 4** *Let  $K$  be a sextic CM-field such that  $h^-(K)$  is odd. Set  $\mathfrak{D} = \mathfrak{D}(K)$ ,  $D = D(K_+)$  and  $d = d(K)$ . Let  $\Lambda \in K$  such that  $\Lambda \notin K_+$  and  $\Lambda$  is not quadratic. Assume also  $L = N_{K/K_+}\Lambda$  is a rational integer.*

If  $\Lambda \in \mathfrak{D}$ , we have

$$L > C'(D, d).$$

Let  $\mathfrak{r}$  be an ideal of  $K_+$  which is free of square factor of ideals from  $K_+$ . Assume  $\mathfrak{r}$  is coprime to the relative discriminant of  $K/K_+$  if  $K = K_+(\sqrt{-1})$ . If  $\Lambda \in \mathfrak{r}\mathfrak{D}$ , we have

$$L > C'(D, (N_{K_+/\mathbf{Q}}\mathfrak{r})^2 d).$$

Let  $\mathfrak{l}$  be a prime ideal of degree 1 of  $K_+$  and  $l$  the prime number contained in  $\mathfrak{l}$ . Assume  $l$  is coprime to  $D$ . Assume also  $l^{-1}$  is coprime to the relative discriminant of  $K/K_+$  if  $K = K_+(\sqrt{-1})$ . If  $\Lambda \in l^{-1}\mathfrak{D}$ , we have

$$L > C(l^2 D, l^4 d).$$

This Lemma is a consequence of the proposition of geometry of numbers that is stated below. Let  $\alpha \in K_+ \mapsto \alpha^{(i)} \in \mathbf{R}$  ( $i = 1, 2, 3$ ) be distinct embeddings of a given totally real cubic field in  $\mathbf{R}$  and  $\alpha \in K_+ \mapsto \vec{\alpha} = {}^t(\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}) \in \mathbf{R}^3$  the Minkowski embedding of  $K_+$ . We decompose a given vector  $\mathbf{x} \in \mathbf{R}^3$  as  $\mathbf{x} = \mathbf{x}_\perp + \mathbf{x}_\parallel$ , where  $\mathbf{x}_\perp$  is orthogonal to  $\vec{1}$  and  $\mathbf{x}_\parallel$  is parallel to  $\vec{1}$ .

**Proposition 5** *Let  $K_+$  be a totally real cubic field and  $\mathfrak{o} = \mathfrak{D}(K_+)$ . If  $\alpha \in \mathfrak{o} \setminus \mathbf{Z}$ , we have*

$$\mathrm{tr}_{K_+/\mathbf{Q}} \alpha^2 = \|\vec{\alpha}\|^2 \geq \|\vec{\alpha}_\perp\|^2 \geq \max \left\{ (2D)^{1/3}, \frac{2}{3}f \right\},$$

where  $D = D(K_+)$  and  $f = f(K_+)$ . If  $1, \alpha, \beta \in \mathfrak{o}$  are linearly independent over  $\mathbf{Q}$ , we have

$$\|\vec{\alpha}_\perp\|^2 \cdot \|\vec{\beta}_\perp\|^2 \geq D/3.$$

Let  $\mathfrak{l}$  be a prime ideal of degree 1 of  $K_+$  and  $l$  the prime number contained in  $\mathfrak{l}$ . Assume  $l$  is coprime to  $D$ . If  $\alpha \in l^{-1} \setminus l\mathbf{Z}$ , we have

$$\mathrm{tr}_{K_+/\mathbf{Q}} \alpha^2 = \|\vec{\alpha}\|^2 \geq \|\vec{\alpha}_\perp\|^2 > (2l^2 D)^{1/3}.$$

If  $l, \alpha, \beta \in l^{-1}$  are linearly independent over  $\mathbf{Q}$ , we have

$$\|\vec{\alpha}_\perp\|^2 \cdot \|\vec{\beta}_\perp\|^2 \geq l^2 D/3.$$

We will give an ideal theoretic proof of the inequality  $\|\alpha_\perp\|^2 \geq 2f/3$ . However, we also give a proof of the inequality  $\|\alpha_\perp\|^2 \geq f/3$  through geometry of numbers, which hopefully illustrates the nature of Proposition 5.

Algebraic properties of CM-fields, whose relative class numbers are odd, are also used in our proof of the Theorems. Some other properties are also important for further study toward determination of sextic CM-fields of (relative) class number one. When a number field  $L$  is given, let  $\mathcal{C}(L)$  be the class group of  $L$ ,  $E(L)$  the group of units of  $L$  and  $W(L)$  the group of roots of unity of  $L$ . When a CM-field  $K$  is given, we denote by  $\kappa(K)$  the order of the kernel of the lifting map  $\mathcal{C}(K_+) \mapsto \mathcal{C}(K)$  of ideal classes. Let  $E^+(K_+)$  the group of totally positive units of  $K_+$ . Hasse's unit index  $[E(K) : E(K_+)W(K)]$  is denoted by  $Q(K)$ . The ideal character of  $K_+$  associated with  $K/K_+$  is denoted by  $\chi_{K/K_+}$ .

The algebraic properties are described in the following:

**Lemma 6** *Let  $K$  be a CM-field such  $h^-(K)$  and  $[K : \mathbf{Q}]$  are odd. Then, the following assertions hold:*

- (i)  $h(K_+)$  is odd;
  - (ii)  $E^+(K_+) = E(K_+)^2$ ;
  - (iii)  $\kappa(K) = 1$ ;
  - (iv)  $Q(K) = 1$ ;
  - (v)  $K/K_+$  is ramified at exactly one prime ideal of  $K_+$ .
- Let  $\mathfrak{q} = \mathfrak{q}(K)$  be the prime ideal of  $K_+$  that is ramified in  $K/K_+$  and  $q = q(K)$  the prime number contained in  $\mathfrak{q}$ .
- (vi)  $K = K_+(\sqrt{-1})$  or there is a totally positive integer  $\delta$  of  $K_+$  such that  $K = K_+(\sqrt{-\delta})$  and the ideal  $\delta\mathfrak{q}^{-1}$  is a square ideal of  $K_+$ ;
  - (vii) The inertia degree  $\deg \mathfrak{q}$  is odd if  $q$  is odd;
  - (viii)  $q \not\equiv 1 \pmod{4}$ .
  - (ix) For an arbitrary prime number  $l$ , we have

$$\chi_{K/K_+}(l\mathfrak{o}) = \left(\frac{-d}{l}\right) = \begin{cases} \left(\frac{-4}{l}\right) & \text{if } K = K_+(\sqrt{-1}) \text{ or } \deg \mathfrak{q} \text{ is even;} \\ \left(\frac{-q}{l}\right) & \text{otherwise,} \end{cases}$$

where  $\mathfrak{o}$  denotes  $\mathfrak{D}(K_+)$  and  $(\bullet/\bullet)$  the Kronecker symbol and  $d = d(K)$ .

**Remark.** All assertions except (ix) hold for any CM-field  $K$  such that  $[K : \mathbf{Q}]$  is odd and  $h^-(K)$  is odd.

The following Lemma discriminates for which sextic CM-fields the Theorems are applicable.

**Lemma 7** *Let  $K$  be a sextic CM-field such that  $h^-(K)$  is odd. Let  $\mathfrak{q} = \mathfrak{q}(K)$ ,  $q = q(K)$ ,  $\mathfrak{o} = \mathfrak{D}(K_+)$ ,  $D_0 = D_0(K_+)$  and  $f = f(K_+)$ . Then,  $K$  contains an imaginary quadratic subfield if and only if one of the following condition holds.*

- (i)  $q\mathfrak{o} = \mathfrak{q}$ ;
- (ii)  $q\mathfrak{o} = \mathfrak{q}^3$  or equivalently  $q \mid f$ ;
- (iii)  $q\mathfrak{o} = \mathfrak{q}\mathfrak{q}_2^2$  for some prime ideal  $\mathfrak{q}_2$  of  $K_+$  such that  $\mathfrak{q} \neq \mathfrak{q}_2$ , or equivalently  $q \mid D_0$  and  $q \nmid f$ .

## 2 Preliminaries

We use a Lemma on quadratic extension and another on cubic field.

**Lemma 8** *Let  $F_{\mathfrak{q}}$  be a finite extension of  $\mathbf{Q}_2$  with the unique prime ideal  $\mathfrak{q}$ ,  $v_{\mathfrak{q}} : F_{\mathfrak{q}}^{\times} \rightarrow \mathbf{Z}$  the additive valuation of  $F_{\mathfrak{q}}$  that is normalized so that  $v_{\mathfrak{q}}(F_{\mathfrak{q}}^{\times}) = \mathbf{Z}$ ,  $K_{\mathfrak{Q}}$  a quadratic extension of  $F_{\mathfrak{q}}$  with the unique prime ideal  $\mathfrak{Q}$ , and  $\chi(K_{\mathfrak{Q}}/F_{\mathfrak{q}}; \bullet)$  the norm residue symbol of  $K_{\mathfrak{Q}}/F_{\mathfrak{q}}$ ,  $\mathfrak{d}$  the relative discriminant of  $\chi(K_{\mathfrak{Q}}/F_{\mathfrak{q}}; \bullet)$  and  $e(\mathfrak{q})$  the ramification index of  $\mathfrak{q}$  in  $F_{\mathfrak{q}}/\mathbf{Q}_2$ . Choose an element  $\delta$  of  $F_{\mathfrak{q}}$  such that  $K_{\mathfrak{Q}} = F_{\mathfrak{q}}(\sqrt{-\delta})$ .*

*If  $v_{\mathfrak{q}}(\delta)$  is odd, we have*

- (i)  $\mathfrak{d} = \mathfrak{q}^{2e(\mathfrak{q})+1}$ .
- (ii)  $\chi(K_{\mathfrak{Q}}/F_{\mathfrak{q}}; 5) = +1$  or  $-1$  according as the inertia degree  $\deg \mathfrak{q}$  of  $\mathfrak{q}$  is even or not.

*If  $v_{\mathfrak{q}}(\delta)$  is even, we have*

- (iii)  $\mathfrak{d} \mid \mathfrak{q}^{2e(\mathfrak{q})}$  and  $v_{\mathfrak{q}}(\mathfrak{d}) \in 2\mathbf{Z}$ .

*Proof.* Assertions (1) and (3) are part of [5, Theorem 10.2.9]. It remains to prove (ii).

We denote by  $\mathfrak{o}$  the ring of integers of  $F_{\mathfrak{q}}$ .

If  $\deg \mathfrak{q}$  is even, then the residue field  $\mathfrak{o}/\mathfrak{q}$  of  $F_{\mathfrak{q}}$  is an extension of  $\mathbf{Q}_2$  of even degree. Hence, there is an  $\alpha \in \mathfrak{o}$  such that  $\alpha^2 + \alpha + 1 \equiv 0 \pmod{\mathfrak{q}}$ . We now calculate  $(1 + 2\alpha)^2 = 1 + 4(\alpha^2 + \alpha) \equiv 5 \pmod{4\mathfrak{q}}$ . Therefore, the character  $\chi(K_{\mathfrak{Q}}/F_{\mathfrak{q}}; \bullet)$  of order 2 takes the value 1 at 5.

We now assume  $\deg \mathfrak{q}$  is odd. Since  $(1+2\alpha)^2 \equiv 1+4(\alpha^2+\alpha) \pmod{4\mathfrak{q}}$  for  $\alpha \in \mathfrak{o}$  and  $\tilde{\alpha} \in \mathfrak{o}/\mathfrak{q} \mapsto \tilde{\alpha}^2 + \tilde{\alpha} \in \mathfrak{o}/\mathfrak{q}$  is 2 to 1, the index  $[(1+4\mathfrak{o})/(1+4\mathfrak{q}) : (1+2\mathfrak{o})^2/(1+4\mathfrak{q})]$  of multiplicative groups is 2. Hence, the character  $\chi(K_{\mathfrak{Q}}/F_{\mathfrak{q}}; \bullet)$  of conductor  $2^{e(\mathfrak{q})+1}$  takes the value  $-1$  on  $(1+4\mathfrak{o}) \setminus (1+2\mathfrak{o})^2(1+4\mathfrak{q})$ . (Note: the conductor and the relative discriminant of a given quadratic extension are equal.)

It now suffice to prove  $5 \notin (1+2\mathfrak{o})^2(1+4\mathfrak{q})$ . Suppose, to the contrary, that  $5 \in (1+2\mathfrak{o})^2(1+4\mathfrak{q})$ . Then, there exists some  $\alpha \in \mathfrak{o}$  such that  $5 \equiv (1+2\alpha)^2 \equiv 1+4(\alpha^2+\alpha) \pmod{4\mathfrak{q}}$ . Thus, we have  $\alpha^2 + \alpha + 1 \equiv 0 \pmod{\mathfrak{q}}$ , which means  $\deg \mathfrak{q}$  is even. The contradiction establishes the Lemma. **qed.**

**Lemma 9** *Let  $K_+$  be a totally real cubic field. Put  $D_0 = D_0(K_+)$ ,  $f = f(K_+)$  and  $\mathfrak{o} = \mathfrak{D}(K_+)$ . 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)  $K_+(\sqrt{D_0})/\mathbf{Q}(\sqrt{D_0})$  is a cyclic cubic extension.

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

### 3 Algebraic structure of CM-fields whose relative class numbers are odd

For proving Lemma 6, we use two Lemmata concerning invariants of CM-fields. One is on indices related with units and capitulation kernel:

**Lemma 10** *Let  $K$  be a CM-field. Then, we have  $\kappa(K), Q(K) \in \{1, 2\}$ . Set  $\mathfrak{o} = \mathfrak{D}(K_+)$ . There are several sufficient conditions for these indices to be 1:*

- (i)  $\kappa(K) = 1$  when  $h(K_+)$  is odd;
- (ii)  $\kappa(K) = 1$  if  $K = K_+(\sqrt{-1})$  and  $2\mathfrak{o}$  is not a square ideal in  $K_+$ ;
- (iii)  $\kappa(K) = 1$  if  $K = K_+(\sqrt{-\delta})$  with  $\delta \in K_+$  and  $\delta\mathfrak{o}$  is not a square of any non-principal ideal in  $K_+$ ;
- (iv)  $Q(K) = 1$  when  $[E^+(K_+) : E(K_+)^2] = 1$ .

*Proof.* By Theorems 4.12 and 10.3 of [18] or Theorem 1 of [9], we have  $\kappa(K), Q(K) \in \{1, 2\}$ . Assertion (i) is then obvious since  $\kappa(K)$  is an order of a subgroup of  $\mathcal{C}(K_+)$ . Assertions (ii) and (iii) are in [9, Thoerem 1]. Assertion (iv) is assertion (c) of [9, Proposition 1]. **qed.**

Another Lemma is a collection of several sufficient conditions for a relative class number of a given CM-field to be even. Denote by  $t(K)$  the number of prime ideals that are ramified in  $K/K_+$ .

**Lemma 11** *Let  $K$  be a CM-field. Then,  $2 \mid h^-(K)$  if one of the following conditions hold:*

- (i)  $t(K) \geq 2$ ;
- (ii)  $t(K) = 1$  and  $[E^+(K_+) : E(K_+)] > 1$ ;
- (iii)  $\kappa(K) = 1$  and  $2 \mid h(K_+)$ ;
- (iv)  $\kappa(K) = 2$  and the 2-Sylow subgroup of  $\mathcal{C}(K_+)$  is non-cyclic.

*Proof.* For convenience of the readers, we give a proof.

Let  $\mathcal{A}(K)$  be the group of ideal classes of  $K$  that are invariant under the complex conjugation. Put  $Q'(K) = [N_{K/K_+} K^\times \cap E(K_+) : E(K_+)^2]$ . Satz 15 of Takagi's fundamental paper [16] evaluates the order  $\#\mathcal{A}(K)$  of  $\mathcal{A}(K)$ :

$$\#\mathcal{A}(K) = 2^{t(K)-1} Q'(K) h(K_+). \quad (1)$$

This formula is called the ambiguous class number formula.<sup>†</sup>

Since  $\#\mathcal{A}(K)/h(K_+)$  divides  $h^-(K)$ , this implies

$$2^{t(K)-1} Q'(K) \mid h^-(K). \quad (2)$$

Thus,  $h^-(K)$  is even when condition (i) is satisfied.

We consider the case in which condition (ii) is satisfied. Elements of  $E^+(K_+)$  are norm-residue at every infinite places in  $K/K_+$ . Hence, the Product Formula implies that they are also norm-residue at the unique prime ideal that is ramified in  $K/K_+$ . Therefore, Hasse's principle implies they are norm from  $K^\times$ . Thus,  $Q'(K) = [E^+(K_+) : E(K_+)] > 1$ . Since the latter index is a power of 2, this inequality and (2) imply  $2 \mid h^-(K)$ .

We now consider the case in which condition (iii) is satisfied. Let  $\mathfrak{a}$  be an ideal in an ideal class of order 2 of  $K_+$  and set  $\mathfrak{D} = \mathfrak{D}(K)$ . Then,  $\mathfrak{a}\mathfrak{D}$  belongs to an ideal class of order 2 of  $K$  since  $\kappa(K) = 1$ . On the other hand,  $N_{K/K_+}(\mathfrak{a}\mathfrak{D}) = \mathfrak{a}^2$  is principal. Therefore, the kernel of the norm map  $N_{K/K_+} : \mathcal{C}(K) \rightarrow \mathcal{C}(K_+)$  has an element of order 2. Noting that the order of this kernel equals  $h^-(K)$ , we now see  $2 \mid h^-(K)$ .

The last case is treated similarly.

**qed.**

*Proof of Lemma 6.* Set  $\mathfrak{o} = \mathfrak{D}(K_+)$ . Define the character  $\chi^\sharp$  by  $\chi^\sharp(\alpha) = \chi(\alpha\mathfrak{o})$  for  $\alpha \in \mathfrak{o}$ . Then,  $\chi^\sharp$  factors as

$$\chi^\sharp(\alpha) = \prod_{\mathfrak{p} \mid \mathfrak{d}} \chi_{\mathfrak{p}}(\alpha) \cdot \text{sgn } N_{K_+/\mathbf{Q}}\alpha, \quad (3)$$

where the ideal  $\mathfrak{d}$  is the relative discriminant of  $K/K_+$ ,  $\chi_{\mathfrak{p}}$  is a character whose conductor is a power of  $\mathfrak{p}$  and the function  $\text{sgn } x$  is the signature of  $x \in \mathbf{R}$ .

Since  $[K_+ : \mathbf{Q}]$  is odd, this implies  $1 = \chi^\sharp(-1) = -\prod_{\mathfrak{p} \mid \mathfrak{d}} \chi_{\mathfrak{p}}(-1)$ , and in particular  $\prod_{\mathfrak{p} \mid \mathfrak{d}} \chi_{\mathfrak{p}}(-1) \neq 1$ . Therefore,  $\mathfrak{d}$  is non-trivial, i.e.,  $t(K) \geq 1$ .

On the other hand,  $h^-(K)$  is odd. Hence, Lemma 11-(i) implies  $t(K) \leq 1$ . Therefore, assertion (v) is established.

Assertion (v) and Lemma 11-(ii) imply assertion (ii). Then, Lemma 10-(iv) implies assertion (iv).

Now, Lemma 11-(iv) implies that the 2-Sylow subgroup of  $\mathcal{C}(K_+)$  is cyclic.

We now show assertion (iii). Suppose  $\kappa(K) \neq 1$ . Then,  $\kappa(K) = 2$  by Lemma 10. Hence,  $2 \mid h(K_+)$  by Lemma 10-(i). The result of the

---

<sup>†</sup>The quotation of (1) in [12] involved an incorrect denominator. The incorrect denominator vanished in the context so that the argument there can be justified.

previous paragraph then implies that there exists a unique non-principal ideal  $\mathfrak{a}$  of  $K_+$ , up to multiplication by an element of  $K_+^\times$ , such that  $\mathfrak{a}^2$  is principal. By assertion (ii), we can take a totally positive element of  $K_+$  which generates  $\mathfrak{a}^2$ . Such an  $\alpha$  is uniquely defined up to multiplication by a square of an element of  $K_+^\times$ . Lemma 10-(iii) now implies that either  $K = K_+(\sqrt{-1})$  or  $K = K_+(\sqrt{-\alpha})$ . We can deduce  $2 \mid h^-(K_+(\sqrt{-1}))$  as follows: the ideal  $2\mathfrak{o}$  cannot be a square in  $K_+$  since  $[K_+ : \mathbf{Q}]$  is even; hence Lemma 10-(ii) implies  $\kappa(K_+(\sqrt{-1})) = 1$ ; therefore Lemma 11-(iii) implies  $2 \mid h^-(K_+(\sqrt{-1}))$ . By this argument, we eliminate the possibility of  $K = K_+(\sqrt{-1})$ . We can also deduce  $2 \mid h^-(K_+(\sqrt{-\alpha}))$  as follows: let  $H$  and  $H_0$  be the respective 2-class field of  $K_+(\sqrt{-1})$  and  $K_+$ ; we have  $H_0(\sqrt{-1}) = K_+(\sqrt{-1})H_0 \subsetneq H$  since  $2 \mid h^-(K_+(\sqrt{-1}))$ ; on the other hand,  $H_0$  contains  $K_+(\sqrt{\alpha})$  by the uniqueness of  $\alpha$ ; thus  $H_0(\sqrt{-1})$  contains  $K_+(\sqrt{-\alpha})$  and equals  $H_0(\sqrt{-\alpha})$ ; moreover,  $H_0(\sqrt{-\alpha})/K_+(\sqrt{-\alpha})$  is unramified since  $H_0/K_+$  is unramified; if  $H/K_+(\sqrt{-\alpha})$  is abelian, then we get  $2 \mid h^-(K_+(\sqrt{-\alpha}))$  from  $H_0(\sqrt{-\alpha}) = H_0(\sqrt{-1}) \subsetneq H$ ; otherwise Burnside Basis Theorem (see e.g. [15, Theorem 1.16 (p. 92)]) implies that  $H/K_+(\sqrt{-\alpha})$  contains an abelian non-cyclic extension  $H_1/K_+(\sqrt{-\alpha})$ ; the extensions  $H_0H_1/K_+(\sqrt{-\alpha})$  is also non-cyclic; this implies  $H_0H_1 \neq H_0(\sqrt{-\alpha})$  since  $\text{Gal}(H_0(\sqrt{-\alpha})/K_+(\sqrt{-\alpha})) \simeq \text{Gal}(H_0/K_+)$  is isomorphic to a cyclic subgroup of  $\mathcal{C}(K_+)$ ; thus  $2 \mid [H_0H_1 : H_0(\sqrt{-\alpha})] \mid h^-(K_+(\sqrt{-\alpha}))$ . Therefore, the possibility of  $K = K_+(\sqrt{-\alpha})$  is also eliminated. We have established assertion (iii).

Assertion (iii), Lemma 11-(iii) and the assumption  $2 \nmid h^-(K)$  imply assertion (i).

Now define  $\mathfrak{q}$  and  $q$  as in the Lemma. Choose  $\delta \in \mathfrak{o}$  so that  $K = K_+(\sqrt{-\delta})$ . Then,  $\delta$  is totally positive. Uniqueness of  $\mathfrak{q}$  implies  $\delta\mathfrak{o}$  or  $\delta\mathfrak{q}^{-1}$  is a square of some ideal  $\mathfrak{a}$  of  $K_+$ . In the latter case, assertion (vi) is obvious. In the former case, assertion (i) implies that  $\mathfrak{a}$  is generated by some  $\alpha \in K_+^\times$ . Hence,  $\alpha^{-2}\delta \in E^+(K_+)$ . Thus, assertion (ii) implies  $\alpha^{-2}\delta = \eta^2$  for some  $\eta \in E(K_+)^2$ . We now get  $K = K_+(\sqrt{-\delta}) = K_+(\sqrt{-\alpha^2\eta^2}) = K_+(\sqrt{-1})$ , establishing assertion (vi).

We now show assertions (vii) and (viii). Recall the factorization (3). Assertion (v) implies

$$\chi^\sharp(\alpha) = \chi_{\mathfrak{q}}(\alpha) \cdot \text{sgn } N_{K_+/\mathbf{Q}}\alpha \quad (4)$$

and hence

$$\chi_{\mathfrak{q}}(-1) = -1. \quad (5)$$

If  $\mathfrak{q}$  is odd, then the character  $\chi_{\mathfrak{q}}$  is the quadratic residue symbol modulo  $\mathfrak{q}$ . Hence, we get

$$-1 = \chi_{\mathfrak{q}}(-1) = \left( \frac{-1}{\mathfrak{q}} \right)_{K_+} = \left( \frac{(-1)^{\deg \mathfrak{q}}}{q} \right).$$

Now, assertions (vii) and (viii) follow.

It remains to show assertion (ix). Let  $q' = q$  if  $\deg \mathfrak{q}$  is odd and  $K \neq K_+(\sqrt{-1})$  or  $q' = 4$  otherwise. By assertion (vii) and Lemma 8, we have  $(-d/l) = (-q'/l)$ . Thus, we prove  $\chi_{K/K_+}(l\mathfrak{o}) = (-q'/l)$ .

Firstly, we discuss the case in which  $K \neq K_+(\sqrt{-1})$  and  $\deg \mathfrak{q}$  is odd. If  $\mathfrak{q}$  is odd, then  $\chi_{\mathfrak{q}}$  equals the quadratic residue symbol modulo  $\mathfrak{q}$ . Therefore, we can calculate

$$\chi(l\mathfrak{o}) = \left( \frac{l}{\mathfrak{q}} \right)_{K_+} = \left( \frac{l^{\deg \mathfrak{q}}}{q} \right) = \left( \frac{l}{q} \right) = \left( \frac{-q}{l} \right).$$

If  $\mathfrak{q}$  is even, Lemma 8 implies that the relative discriminant  $\mathfrak{d}$  divides  $8\mathfrak{o}$  and  $\chi_{\mathfrak{q}}(5) = -1$ . Recalling (5), we deduce the assertion.

Secondly, we discuss the case in which  $K = K_+(\sqrt{-1})$ . Lemma 8 implies that  $\mathfrak{d}$  divides  $4\mathfrak{o}$ . Hence, (5) implies the assertion.

Lastly, we discuss the case in which  $K \neq K_+(\sqrt{-1})$  and  $\deg \mathfrak{q}$  is even. By assertion (vii), we see  $q = 2$  and, by assertion (vi),  $K = K(\sqrt{-\delta})$  for some  $\delta \in K_+$  such that  $\delta\mathfrak{q}^{-1}$  is a square of some ideal of  $K_+$ . By using Lemma 8, we can now calculate

$$\chi_{\mathfrak{q}}(5\mathfrak{o}) = +1 \tag{6}$$

On the other hand, Lemma 8 implies that  $\mathfrak{d}$  divides  $8\mathfrak{o}$ . Therefore, the identities (5) and (6) imply the assertion. **qed.**

*Proof of Lemma 7.* We firstly assume  $K$  contains a quadratic subfield  $k$  and show one of the conditions (i), (ii) and (iii) holds.

Denote by  $e(M/M_0, \mathfrak{P})$  the ramification index of a given prime ideal  $\mathfrak{P}$  of  $M$  in a given extension  $M/M_0$  of number fields. Let  $\mathfrak{Q}$  be the prime ideal of  $K$  above  $\mathfrak{q}$ . By Lemma 6-(v), we have  $e(K/K_+, \mathfrak{P}) = 1$  for every prime ideals  $\mathfrak{P} \neq \mathfrak{Q}$  of  $K$ . On the other hand,  $e(K/\mathbf{Q}, \mathfrak{P})$  is even for every prime ideal  $\mathfrak{P}$  of  $K$  above  $q$ . Therefore, we get  $e(K_+/\mathbf{Q}, \mathfrak{p}) = 2$  for every prime ideal  $\mathfrak{p} \neq \mathfrak{q}$  of  $K_+$  above  $q$ . Therefore, one of the conditions (i), (ii) and (iii) holds.

We secondly assume one of conditions (i), (ii) and (iii) and show that  $K$  contains an imaginary quadratic subfield. By Lemma 6-(vi),  $K = K_+(\sqrt{-1})$

or  $K = K_+(\sqrt{-\delta})$  with a totally positive element  $\delta$  of  $K_+$  such that  $\delta\mathfrak{q}^{-1}$  is a square ideal in  $K_+$ . The former case is trivial. In the latter case, we note  $q\mathfrak{q}^{-1}$  is a square ideal in  $K_+$  under our assumption. Therefore,  $q^{-1}\delta\mathfrak{D}(K_+)$  is a square ideal in  $K_+$ . By Lemma 6-(i), this implies  $q^{-1}\delta = \alpha^2\varepsilon$  for some  $\alpha \in K_+^\times$  and  $\varepsilon \in E(K_+)$ . Since the left hand side is totally positive, the unit  $\varepsilon$  is also totally positive. By Lemma 6-(ii), this imply  $\varepsilon = \eta^2$  for some  $\eta \in E(K_+)$ . Therefore, we conclude  $K = K_+(\sqrt{-\delta}) = K_+(\sqrt{-q\alpha^2\eta^2}) = K_+(\sqrt{-q})$  and  $K$  contains an imaginary quadratic subfield.  $\quad \mathbf{qed.}$

## 4 Geometric structure of sextic CM-fields whose relative class numbers are odd

Denote by  $D({}^t(x_1, x_2, x_3))$  the difference-product  $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$  and by  $D(\alpha)$  the discriminant  $D(\vec{\alpha})$  of  $\alpha$  when  $\alpha$  belongs to a totally cubic field  $K_+$ . Obviously,  $D(\alpha)$  is positive if  $\alpha \in K_+ \setminus \mathbf{Q}$ .

For proving Proposition 5, we need the following:

**Lemma 12** *Let  $K_+$  be a totally real cubic field. Let  $\mathfrak{l}$  be a prime ideal of degree 1 of  $K_+$  and  $l$  the prime number contained in  $\mathfrak{l}$ . Assume  $l$  is coprime to  $D = D(K_+)$ . If  $\alpha \in \mathfrak{l}^{-1} \setminus l\mathbf{Z}$ , we have*

$$D(\alpha) \geq l^2 D.$$

*Proof.* We have

- (a)  $K_+$  is cyclic and  $l$  splits completely in  $K_+$ ;
- (b)  $K_+$  is non-normal and  $l$  splits completely in  $K_+$ ; or
- (c)  $K_+$  is non-normal and  $l$  does not split completely in  $K_+$ .

We discuss case (b). The other cases are easier.

Let  $D_0 = D_0(K_+)$  and  $M = K_+(\sqrt{D_0})$ . Then,  $M$  is the normal closure of  $K_+$ .

Let  $\tau$  be the non-trivial conjugation of  $M/K_+$  and  $\rho$  be a generator of  $\text{Gal}(M/\mathbf{Q}(\sqrt{D_0}))$ . We have  $\tau^{-1}\rho\tau = \rho^{-1}$ .

By Lemma 9, complete splitting of  $l$  in  $K_+/\mathbf{Q}$  implies  $(D_0/l) = +1$ . Thus,  $l$  splits completely in  $M/\mathbf{Q}$ . Let  $\mathfrak{L}_1$  be a prime ideal above  $\mathfrak{l}$ . Set  $\mathfrak{L}_2 = \mathfrak{L}_1^\rho$  and  $\mathfrak{L}_3 = \mathfrak{L}_1^{\rho^2}$ . Then, we have  $\alpha \in \mathfrak{L}_2\mathfrak{L}_3\mathfrak{L}_2^\tau\mathfrak{L}_3^\tau$ .

We can now verify  $\alpha^\rho \in \mathfrak{L}_3 \mathfrak{L}_1 \mathfrak{L}_1^\tau \mathfrak{L}_2^\tau$  and  $\alpha - \alpha^\rho \in \mathfrak{L}_3 \mathfrak{L}_2^\tau$ . Noting that  $D(\alpha) = -N_{M/\mathbf{Q}}(\alpha - \alpha^\rho)$ , we now see  $l^2 \mid D(\alpha)$ . On the other hand, we know  $D \mid D(\alpha)$ . Since  $l$  is coprime to  $D$ , these imply  $l^2 D \mid D(\alpha)$ .

Since  $\alpha \in K_+ \setminus \mathbf{Q}$  this implies the assertion. **qed.**

*Proof of Proposition 5.* Obviously, we have  $\text{tr}_{K_+/\mathbf{Q}} \alpha^2 = \|\vec{\alpha}\|^2 \geq \|\vec{\alpha}_\perp\|^2$ .

We firstly prove  $\|\vec{\alpha}_\perp\|^2 \geq (2D)^{1/3}$ . Satz II of [14] implies  $\|\vec{\alpha}_\perp\|^2 \geq (2D(\vec{\alpha}_\perp))^{1/3} = (2D(\alpha))^{1/3}$ . The equality requires  $\alpha^{(i)} = \alpha^{(i+1)} = -\alpha^{(i+2)}/2$  for some  $i \in \{1, 2, 3\}$ . (The super scripts is read modulo 3.) This is impossible for a cubic number. Hence, the equality sign can be removed. (See Remark A.) Substituting  $D(\alpha) \geq D$ , we see  $\|\vec{\alpha}_\perp\|^2 \geq (2D)^{1/3}$ .

We secondly prove  $\|\vec{\alpha}_\perp\|^2 \geq 2f/3$ . Let  $X^3 - aX + bX - c$  be the minimal polynomial of  $\alpha$ . We have  $0 < \|\vec{\alpha}_\perp\|^2 = \|\vec{\alpha}\|^2 - \|(a/3)\vec{1}\|^2 = (2/3)(a^2 - 3b)$ . Thus, it suffice to prove  $f \mid a^2 - 3b$ .

We write  $\vec{\alpha} = {}^t(\alpha_1, \alpha_2, \alpha_3)$ , identify  $K_+$  with  $\mathbf{Q}(\alpha_1)$  by  $\alpha \mapsto \alpha_1$  and regard  $M = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$  as the normal closure of  $K_+$ . Let  $\Delta = \alpha_2 - \alpha_3$ . Then, we have  $\Delta^2 = a^2 - 2b - \alpha_1^2 - 2c/\alpha_1 \in K$  and  $D(\alpha) = N_{K_+/\mathbf{Q}}\Delta^2$ .

For each prime number  $p$  dividing  $f$ , we consider the prime ideal  $\mathfrak{p}$  of  $K_+$  above  $p$  and show  $\Delta^2 \in \mathfrak{p}^{2j}$ , where  $j$  denotes the largest integer such that  $p^j \mid f$ . Such a prime number  $p$  is totally ramified in  $K_+/\mathbf{Q}$  by Lemma 9-(i). Hence,  $N_{K_+/\mathbf{Q}}\mathfrak{p} = p$ . Therefore, we can infer

$$p^j \mid f \implies p^{2j} \mid D \implies p^{2j} \mid D(\alpha) = N_{K_+/\mathbf{Q}}\Delta^2 \implies \Delta^2 \in \mathfrak{p}^{2j}.$$

In particular, we get

$$\Delta \in \tilde{\mathfrak{p}}^j, \tag{7}$$

where  $\tilde{\mathfrak{p}} = \mathfrak{p}\mathfrak{D}(M)$ . (The ideal  $\tilde{\mathfrak{p}}$  is not necessarily a prime ideal of  $M$ .)

Since  $\tilde{\mathfrak{p}}$  is Galois invariant, this implies  $\alpha_1 \equiv \alpha_2 \equiv \alpha_3 \pmod{\tilde{\mathfrak{p}}^j}$ .

A particular consequence of this congruence is the following:

$$a^2 - 3b = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_2\alpha_3 - \alpha_3\alpha_1 \in \tilde{\mathfrak{p}}.$$

If  $j = 1$ , this implies  $p^j \mid a^2 - 3b$  as desired.

Assume  $j \geq 2$ . Then, we have  $p = 3$  and  $j = 2$  by Lemma 9-(vi). If we write  $\Delta_1 = \Delta = \alpha_2 - \alpha_3$ ,  $\Delta_2 = \alpha_3 - \alpha_1$  and  $\Delta_3 = \alpha_1 - \alpha_2$ , Galois invariance of  $\tilde{\mathfrak{p}}$  and claim (7) implies  $\Delta_1, \Delta_2, \Delta_3 \in \tilde{\mathfrak{p}}^j = \tilde{\mathfrak{p}}^2$ . Therefore, we get

$$2(a^2 - 3b) = \Delta_1^2 + \Delta_2^2 + \Delta_3^2 \in \tilde{\mathfrak{p}}^4$$

and hence  $p^2 \mid 2(a^2 - 3b)$ . Noting  $p = 3$  is odd, we now see  $p^j \mid a^2 - 3b$ .

We have established the first assertion.

We thirdly prove  $\|\vec{\alpha}_\perp\|^2 \cdot \|\vec{\beta}_\perp\|^2 \geq D/3$ . Let  $\mathfrak{o} = \mathfrak{O}(K_+)$ . We calculate the determinant  $\left| \vec{1}, \vec{\alpha}_\perp, \vec{\beta}_\perp \right|^2$  as follows:

$$\left| \vec{1}, \vec{\alpha}_\perp, \vec{\beta}_\perp \right|^2 = \left| \vec{1}, \vec{\alpha}, \vec{\beta} \right|^2 = [\mathfrak{o} : \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta]^2 D.$$

Neglecting the index and using Hadamard inequality, we get the desired inequality.

We nextly prove the third assertion. By Lemma 12, we have  $D(\alpha) \geq l^2 D$ . Thus, we can replace  $D$  of the first paragraph of this proof with  $l^2 D$ , establishing the third assertion.

We now prove the last assertion. We have

$$\left| \vec{l}, \vec{\alpha}_\perp, \vec{\beta}_\perp \right|^2 = \left| \vec{l}, \vec{\alpha}, \vec{\beta} \right|^2 = [\mathfrak{o} : \mathbf{Z}l + \mathbf{Z}\alpha + \mathbf{Z}\beta]^2 D.$$

Here, the index is larger than  $N_{K_+/\mathbf{Q}}(ll^{-1}) \geq l^2$  since  $l, \alpha, \beta \in ll^{-1}$  and  $l, \alpha, \beta$  are linearly independent over  $\mathbf{Q}$ . The last assertion follows immediately.

**qed.**

**Remark A.** We give here an alternative proof of  $\|\vec{\alpha}_\perp\|^2 \geq (2D(\alpha))^{1/3}$ . Put  $\omega = \alpha - \text{tr}_{K_+/\mathbf{Q}} \alpha / 3$ . Then,  $\|\vec{\alpha}_\perp\| = \|\vec{\omega}\|$ . The minimal polynomial of  $\omega$  is of the form  $X^3 - bX - c'$ , where  $b \in (1/9)\mathbf{Z}$  and  $0 \neq c' \in (1/27)\mathbf{Z}$ . We have  $\|\vec{\alpha}_\perp\|^2 = \text{tr}_{K_+/\mathbf{Q}} \omega^2 = 2b'$ . On the other hand, we have  $D(\alpha) = D(\omega) = 4(b')^3 - 27(c')^2$ . Therefore, we get

$$\|\vec{\alpha}_\perp\|^2 = (2D(\alpha) + 54(c')^2)^{1/3} \geq (2D(\alpha) + 2/27)^{1/3} > (2D(\alpha))^{1/3}$$

as desired.

**Remark B.** A weaker inequality  $\|\vec{\alpha}_\perp\|^2 \geq f/3$  can be proved in a more geometrical way. We have  $\sqrt{D_0}\Delta \in K_+$ . The minimal polynomial of  $\sqrt{D_0}\Delta$  is

$$X^3 - D_0(a^2 - 3b)X \pm D_0\sqrt{D_0D(\alpha)}.$$

We set  $\vec{\Delta} = {}^t(\Delta_1, \Delta_2, \Delta_3) = \vec{\alpha} \times \vec{1}$ . Then,  $\|\sqrt{D_0}\vec{\Delta}\|^2 = 2D_0(a^2 - 3b) = 3D_0\|\vec{\alpha}_\perp\|^2$ . Hence, we can calculate

$$D \leq \left| \vec{1}, \vec{\alpha}, \sqrt{D_0}\vec{\Delta} \right|^2 = \left| \vec{1}, \vec{\alpha}_\perp, \sqrt{D_0}\vec{\Delta} \right|^2 \leq 3\|\vec{\alpha}_\perp\|^2 \cdot \|\sqrt{D_0}\vec{\Delta}\|^2 = D_0(3\|\vec{\alpha}_\perp\|)^2$$

by using Hadamard inequality. The desired inequality now follows on noting  $D = D_0 f^2$ .

**Remark C.** Remark A suggests that the inequality  $\|\vec{\alpha}_\perp\|^2 \geq (2D(\alpha))^{1/3}$  is the best possible lower bound of  $\|\vec{\alpha}_\perp\|^2$  in terms of the discriminant  $D$  of  $\mathbf{Q}(\alpha)$ . Indeed, Erdős [6] proved  $g(n)$  ( $0 \leq n \in \mathbf{Z}$ ) is infinitely often free of  $m$ -th power when  $g(X)$  is a polynomial of degree  $m+1 \geq 3$  with integer coefficients, the greatest common divisor of the coefficients of  $g(X)$  is 1 and there exists some  $n_0 \in \mathbf{Z}$  such that  $g(n_0) \not\equiv 0 \pmod{2^m}$ . This can be applied to the polynomial  $g(X) = 4X^3 - 27$  and  $m = 2$ . Therefore, the discriminant  $4b^3 - 27$  of the polynomial  $X^3 - bX - 1$ , with  $2 < b \in \mathbf{Z}$ , is infinitely often free of square factor. (For example  $4 \cdot 2003^3 - 27 = 32144216081$  is a prime number.) In this situation, the discriminant  $D(\alpha)$  of its root coincides with  $D$ . We then have  $\|\vec{\alpha}\|^2 = 2b = (2D + 52)^{1/3}$ .

**Remark D.** The inequality  $\|\vec{\alpha}_\perp\|^2 \geq 2f/3$  has some suggestion on the polynomial  $4X^3 - 27$ . When  $4b^3 - 27$  coincides with the discriminant  $D$  of the field defined by  $X^3 - bX - 1$ , this inequality implies  $(2D + 54)^{1/3} \geq 2f/3$ . Here,  $f$  equals  $\sqrt{D/D_1}$  or  $2\sqrt{D/D_1}$  with square-free part  $D_1$  of  $D$ . We get  $D_1 > (D/4)^{1/3}/9 - \epsilon$ . Numerical examples a similar inequality, with smaller exponent, should hold even in the case  $D \neq 4b^3 - 27$ . However, its proof is beyond the method of this paper.

If  $K$  is a CM-field, there is a totally positive element  $\delta$  of  $K_+$  such that  $K = K_+(\sqrt{-\delta})$ . A unique non-trivial automorphism of  $K/K_+$  is induced by  $\sqrt{-\delta} \mapsto -\sqrt{-\delta}$ . This automorphism is called the complex conjugation of  $K$ . We denote it by  $\sigma = \sigma_K$ .

*Proof of Lemma 4.* Write  $\Lambda = (\alpha + \sqrt{-\beta})/2$  with  $\alpha, \beta \in \mathfrak{D}(K_+)$ . Then, the integer  $\beta$  of  $K_+$  is totally positive. Put  $L = N_{K/K_+}\Lambda \in \mathbf{Q}$ . Then, we have

$$4L = \alpha^2 + \beta. \quad (8)$$

The integer  $\alpha$  of  $K_+$  is irrational. Suppose  $\alpha \in \mathbf{Q}$ . Then,  $\beta = 4L - \alpha^2 \in \mathbf{Q}$  by (8). Thus,  $\Lambda$  is quadratic, which contradicts the assumption of the Lemma.

The integers 1,  $\alpha$  and  $\beta$  of  $K_+$  are linearly independent over  $\mathbf{Q}$ . Suppose they are linearly dependent. Then,  $\beta = a\alpha + c$  for suitable  $a, c \in \mathbf{Q}$ . Substituting this in (8), we get  $\alpha^2 + a\alpha + c - 4g = 0$ . Hence, the degree of  $\alpha$  is at most 2. Since  $K_+$  is a cubic field, this implies  $\alpha \in \mathbf{Q}$ , which is impossible as we have seen.

Let  $b = \text{tr}_{K/K_+} \beta$  and put  $\beta_i = \beta^{(i)}$  ( $i = 1, 2, 3$ ). Then, we have

$$b > \sqrt{\frac{3}{2}\|\vec{\beta}_\perp\|^2 + B}, \quad (9)$$

where  $B$  denotes  $9(N_{K_+/\mathbf{Q}}\beta)^{2/3}$ . Indeed, we have  $\|\beta_\perp\|^2 = \|\vec{\beta}\|^2 - \|\vec{\beta}_\parallel\|^2 = \|\vec{\beta}\|^2 - b^2/3 = (2/3)(\beta_1^2 + \beta_2^2 + \beta_3^2 - \beta_1\beta_2 - \beta_2\beta_3 - \beta_3\beta_1) = (2/3)(b^2 - 3\beta_1\beta_2 - 3\beta_2\beta_3 - 3\beta_3\beta_1)$  since  $\vec{\beta}_\parallel = (b/3)\vec{1}$ . Therefore, we get  $b^2 = (3/2)\|\vec{\beta}_\perp\|^2 + 3\beta_1\beta_2 + 3\beta_2\beta_3 + 3\beta_3\beta_1$ . Now, the inequality of arithmetic and geometric means implies (9). Here, the equality is eliminated by the fact  $\beta^{-1}N_{K_+/\mathbf{Q}}\beta$  is irrational, which follows from linear independence of  $1, \alpha$  and  $\beta$  over  $\mathbf{Q}$ .

The inequality (9) implies

$$12L = \text{tr}_{K_+/\mathbf{Q}}(\alpha^2 + \beta) > \|\vec{\alpha}_\perp\|^2 + \sqrt{\frac{3}{2}\|\vec{\beta}_\perp\|^2 + B} \geq \Phi(\|\vec{\alpha}_\perp\|^2), \quad (10)$$

where the function  $\Phi(x)$  of  $x > 0$  is defined by

$$\Phi(x) = x + \sqrt{\frac{3\|\vec{\alpha}_\perp\|^2\|\vec{\beta}_\perp\|^2}{2x} + B}.$$

Define the function  $\Phi(A, B; x)$  by

$$\Phi(A, B; x) = x + \sqrt{\frac{A}{2x} + B}$$

so that  $\Phi(x) = \Phi(3\|\vec{\alpha}_\perp\|^2\|\vec{\beta}_\perp\|^2, B; x)$ . Then, we have

$$\frac{d\Phi(A, B; x)}{dx} = \frac{4x^2\sqrt{A/2x+B} - A}{4x^2\sqrt{A/2x+B}} > \frac{\left((2x)^{3/2} - \sqrt{A}\right)\sqrt{A}}{4x^2\sqrt{A/2x+B}} > 0 \quad (11)$$

for  $x > A^{1/3}/2$ . Obviously, we also have  $\Phi(x) \geq \Phi(A, B; x) \geq \Phi(A_0, B_0; x)$  when  $A \geq A_0 > 0$  and  $B \geq B_0 > 0$ .

We now prove the first assertion. Proposition 5 is applicable since  $1, \alpha$  and  $\beta$  are linearly independent over  $\mathbf{Q}$ . Hence, we have  $3\|\vec{\alpha}_\perp\|^2\|\vec{\beta}_\perp\|^2 \geq D$  and hence  $\Phi(\|\vec{\alpha}_\perp\|^2) \geq \Phi(D, B; \|\vec{\alpha}_\perp\|^2)$ .

The inequality (10) and monotonousness (11) imply

$$L > \Phi\left(D, B; (2D)^{1/3}\right) \quad (12)$$

in general and

$$L > \Phi(D, B; 2f/3) \quad (13)$$

if  $2f/3 \geq \sqrt[3]{2D}$ .

On the other hand, we have

$$B \geq 9d^{2/3}. \quad (14)$$

Indeed,  $\beta = N_{K/K_+}(\Lambda - \Lambda^\sigma)$  belongs to the relative discriminant  $\mathfrak{d}$  of  $K/K_+$ . Therefore,  $N_{K_+/\mathbf{Q}}\beta$  is a multiple of  $d = N_{K_+/\mathbf{Q}}\mathfrak{d}$ . The linear independence of 1,  $\alpha$  and  $\beta$  implies  $\beta \neq 0$  and hence  $N_{K_+/\mathbf{Q}}\beta \neq 0$ . Therefore, we get  $N_{K_+/\mathbf{Q}}\beta \geq d$  and hence  $B \geq 9d^{2/3}$ .

Inequalities (12), (13) and (14) imply  $L \geq C'(D, d)$ .

We nextly prove the second assertion. We can follow our proof of the first assertion if we show

$$\beta \in \mathfrak{d}\mathfrak{r}^2. \quad (15)$$

Since  $\mathfrak{r}$  is free of square factors of ideals from  $K_+$ , it suffice to show this divisibility for the case in which  $\mathfrak{r}$  is a prime ideal of  $K_+$ .

Since  $\Lambda \in \mathfrak{r}\mathfrak{D}$  and  $\mathfrak{r}\mathfrak{D}$  is invariant under the complex conjugation, we have  $\sqrt{-\beta} = \Lambda - \Lambda^\sigma \in \mathfrak{r}\mathfrak{D}$ . Hence, we get  $\beta \in \mathfrak{r}^2$ .

If  $\mathfrak{r}$  is coprime to  $\mathfrak{d}$ , this immediately implies (15).

If  $\mathfrak{r}$  divides  $\mathfrak{d}$ , the assumption  $K \neq K_+(\sqrt{-1})$  becomes active. Hence Lemma 6-(v) and (vi) imply that the order of  $\mathfrak{r} = \mathfrak{q}(K)$  in  $\beta$  is odd.

If  $\mathfrak{r}$  divides  $\mathfrak{d}$  and  $\mathfrak{r}$  is an odd ideal, then  $\beta \in \mathfrak{r}^2$  implies (15) since the order of  $\mathfrak{r}$  in  $\beta$  is odd.

If  $\mathfrak{r}$  divides  $\mathfrak{d}$  and  $\mathfrak{r}$  is an even ideal, we can argue as follows: Since  $\Lambda \in \mathfrak{r}$ , we have  $L = N_{K/K_+}\Lambda \in \mathfrak{r}^2$ . Recalling (8), we get  $\alpha^2 + \beta \equiv 0 \pmod{4\mathfrak{r}^2}$ . On the other hand, we have  $\mathfrak{d} \mid 4\mathfrak{r}$  by Lemma 8. Thus, we see

$$\alpha^2 + \beta \equiv 0 \pmod{\mathfrak{d}\mathfrak{r}}. \quad (16)$$

Since the order of  $\mathfrak{r}$  in  $\beta$  is odd, the congruence (16) implies  $\alpha^2, \beta \in \mathfrak{d}\mathfrak{r}$ . Since the order of  $\mathfrak{r} = \mathfrak{q}(K)$  in  $\mathfrak{d}$  is odd by Lemma 8, we get (15) from  $\beta \in \mathfrak{d}\mathfrak{r}$ .

We now prove the last assertion. Since  $l$  is coprime to  $D$ , the ideal  $l\mathfrak{r}^{-1}$  is free of square factors of ideals from  $K_+$ . Thus, we set  $\mathfrak{r} = l\mathfrak{r}^{-1}$ . As we have seen in our proof for the second assertion, the norm  $N_{K_+/\mathbf{Q}}\beta$  is a multiple of  $(N_{K_+/\mathbf{Q}}\mathfrak{r})^2d = l^4d$ . In particular, we have

$$B \geq 9(l^4d)^{2/3}.$$

On the other hand, Proposition 5 implies

$$\mathrm{tr}_{K_+/\mathbf{Q}}\alpha^2 \geq (2l^2D)^{1/3}, \quad \|\vec{\alpha}_\perp\|^2 \cdot \|\vec{\beta}_\perp\|^2 \geq l^2D/3.$$

We can now follow the proof of the first assertion.

**qed.**

## 5 Proof of the Theorems

For proving Theorem 2 and 3, we also use the following:

**Lemma 13** *Let  $K$  be a CM-field such that  $\kappa(K) = 1$ . Let  $\mathfrak{l}$  be a prime ideal of  $K_+$  which does not remain inertia in  $K/K_+$ . Then, we have*

$$N_{K_+/\mathbf{Q}}\mathfrak{l} \geq \frac{1}{2^{[K:\mathbf{Q}]}} \frac{D(K)}{D(K_+)^2}$$

*Proof.* This is Theorem 6 of [10]. (This is of more algebraic nature.) **qed.**  
*Proof of Theorem 3.* Let  $\mathfrak{L}$  be a prime ideal of  $K$  above  $\mathfrak{l}$  and  $\mathfrak{D} = \mathfrak{D}(K)$ .

The first assertion is a direct consequence of Lemma 13.

We prove the second assertion. We discuss the lower bounds of the last case since the other cases are handled in the same way.

The lower bound for  $l^2$  is proved as follows. Put  $\mathfrak{A} = \mathfrak{l}^{-1}\mathfrak{L}^2$  and  $L = l^2$ . Then  $\mathfrak{A}$  is an integral ideal of  $K$  and we have

$$L\mathfrak{D} = \mathfrak{A}\mathfrak{A}^\sigma.$$

This is equivalent to

$$L\mathfrak{o} = N_{K/K_+}\mathfrak{A}.$$

The assumption of the Theorem on the relative class number implies that the norm map from  $\mathcal{C}(K)$  to  $\mathcal{C}(K_+)$  is injective. Hence, the above equality implies that  $\mathfrak{A}$  is principal. Let  $\Lambda'$  be a generator of  $\mathfrak{A}$ . Then, we have

$$N_{K/K_+}\Lambda' = L\varepsilon$$

for some  $\varepsilon \in E(K_+)$ . However, the left hand side is totally positive. Therefore, we get  $\varepsilon \in E^+(K_+)$ . By Lemma 6-(ii), this implies  $\varepsilon = \eta^2$  for some  $\eta \in E(K_+)$ . Put  $\Lambda = \Lambda'\eta^{-1}$ . We now have

$$N_{K/K_+}\Lambda = L.$$

Note that  $\Lambda$  cannot be quadratic since  $K$  contains no imaginary quadratic subfield by assumption and the cubic field  $K_+$  contains no real quadratic subfield for the obvious reason. Note also splitting of  $\mathfrak{l}$  in  $K/K_+$  implies  $\mathfrak{A}$  is not a lift of any ideal from  $K_+$ , which implies  $\Lambda \notin K_+$ . Therefore, Lemma 4 and the previous equality imply  $l^2 > C'(D, l^4d)$ . If we estimate  $l$  by the first

assertion, we get  $l^2 > C'(D, d^5/2^{24})$ . If we estimate  $l$  trivially by  $l > 1$ , we get  $l^2 > C'(D, d)$ .

The lower bound for  $l^{4/3}$  is proved as follows. Put  $\mathfrak{A} = \mathfrak{L}^2 \mathfrak{l}_2 \mathfrak{l}_3$  and  $L = l^2$ . Then, we have  $\mathfrak{A} \subset \mathfrak{l}_2 \mathfrak{l}_3 \mathfrak{D} = \mathfrak{l}^{-1} \mathfrak{D}$ . The prime number  $l$  is coprime to  $D$  since it splits completely in  $K_+/\mathbf{Q}$  (see Lemma 9). We follow our proof of the lower bound for  $l^2$  to find a generator  $\Lambda$  of  $\mathfrak{A}$  such that  $N_{K/K_+} \Lambda = L$ . The generator  $\Lambda$  is not quadratic and is outside  $K_+$  as before. Therefore, Lemma 4 implies  $l^2 = L > C(l^2 D, l^4 d)$ . Hence, we get

$$l^{4/3} > C(D, l^2 d).$$

If we estimate  $l$  by the first assertion, we get  $l^{4/3} > C(D, d^3/2^{12})$ . If we estimate  $l$  trivially by  $l > 1$ , we get  $l^{4/3} > C(D, d)$ .

The third assertion follows from the second assertion as follows. In the first three cases of the second assertion, we have  $l > C'(D, d) > d^{1/3}/4$ . Thus, we get  $l^2 > C'(D, d) d^{1/3}/4 > C'(D, d^2/2^6)$ . In the remaining cases, we can show  $l^2 > C'(D, l^{\deg l} d)$  following our proof of the second assertion. Hence, we get  $l^2 \geq C'(D, d^2/2^6)$  by estimating  $l$  by the first assertion.

We prove the last assertion before the fourth assertion. If every prime ideal of  $K_+$  above  $l$  splits in  $K/K_+$ , the ideal  $l\mathfrak{D}$  of  $K$  becomes a product of two ideals:

$$l\mathfrak{D} = \mathfrak{A}\mathfrak{A}^\sigma,$$

where  $\mathfrak{A} \subset \mathfrak{l}$  and  $\mathfrak{A} \not\subset \mathfrak{l}^\sigma$ . We put  $L = l$  and follow our proof of the second assertion.

It remains to prove the fourth assertion. Let  $\mathfrak{q} = \mathfrak{q}(K)$ . Then,  $\mathfrak{l}$  and  $\mathfrak{q}$  are prime ideals above  $l = q$ . Since their behaviour in  $K/K_+$  are different, they are different prime ideals. On the other hand, there are at most two prime ideals above  $l$  since  $l$  does not split completely in the cubic extension  $K_+/\mathbf{Q}$ . Therefore, we have  $l\mathfrak{o} = \mathfrak{l}\mathfrak{q}^2$ ,  $l^2\mathfrak{q}$ , or  $\mathfrak{l}\mathfrak{q}$ . Let  $\mathfrak{Q}$  be the prime ideal of  $K$  above  $\mathfrak{q}$ . We set  $\mathfrak{A} = \mathfrak{L}\mathfrak{q} = \mathfrak{L}\mathfrak{Q}^2$ ,  $\mathfrak{A} = \mathfrak{L}^2\mathfrak{Q}$  or  $\mathfrak{A} = \mathfrak{L}\mathfrak{Q}$  according to the three cases. We also set  $L = l$ . We can then follow our proof of the second assertion. **qed.**

*Proof of Theorem 2.* Exactly one prime ideal  $\mathfrak{q} = \mathfrak{q}(K)$  of  $K_+$  is ramified in  $K/K_+$  by Lemma 6-(v). By Lemma 6-(vi), (vii) and Lemma 8, the ratio  $d/q'$  is a square in  $\mathbf{Z}$ .

Let  $\chi_{K/K_+}$  be the ideal character of  $K_+$  associated with  $K/K_+$ . Then, by Lemma 6-(ix) we have

$$\chi_{K/K_+}(l\mathfrak{o}) = \left( \frac{-q'}{l} \right).$$

We prove the first assertion. By the condition  $(D/l) = -1$  and Lemma 9-(iii), the prime number  $l$  splits as  $l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2$ , where  $\mathfrak{l}_1$  and  $\mathfrak{l}_2$  are prime ideals of  $K_+$  such that  $\deg \mathfrak{l}_1 = 1$  and  $\deg \mathfrak{l}_2 = 2$ .

Since  $(-q'/l) = -1$ , we can calculate

$$\chi_{K/K_+}(\mathfrak{l}_1\mathfrak{l}_2) = \chi_{K/K_+}(l\mathfrak{o}) = \left(\frac{-q'}{l}\right) = -1.$$

Let  $\mathfrak{l} = \mathfrak{l}_1$  and  $\mathfrak{l}' = \mathfrak{l}_2$  if  $\chi_{K/K_+}(\mathfrak{l}_1) = 1$  or  $\mathfrak{l} = \mathfrak{l}_2$  and  $\mathfrak{l}' = \mathfrak{l}_1$  otherwise. Then, the above equality implies

$$\chi_{K/K_+}(\mathfrak{l}) = +1,$$

i.e.,  $\mathfrak{l}$  splits in  $K/K_+$ . (Unfortunately,  $\mathfrak{l}'$  remains inertia in  $K/K_+$  since  $\chi_{K/K_+}(\mathfrak{l}') = -1$ .)

Now, the first two assertions of Theorem 3 imply the desired assertion.

We prove the second assertion. By Lemma 9-(i) and (ii), we have

$$l\mathfrak{o} = \mathfrak{l}_1^3$$

with a prime ideal  $\mathfrak{l}_1$  of  $K_+$  or

$$l\mathfrak{o} = \mathfrak{l}_1\mathfrak{l}_2^2,$$

with distinct prime ideals  $\mathfrak{l}_1$  and  $\mathfrak{l}_2$  of  $K_+$ . Set  $\mathfrak{l} = \mathfrak{l}_1$ . Set  $\mathfrak{l}' = \mathfrak{l}_1$  in the former case or  $\mathfrak{l}' = \mathfrak{l}_2$  in the latter case.

Since  $(-q'/l) = +1$ , we can calculate

$$\chi_{K/K_+}(\mathfrak{l}(\mathfrak{l}')^2) = \chi_{K/K_+}(l\mathfrak{o}) = \left(\frac{-q'}{l}\right) = +1.$$

Hence, we get

$$\chi_{K/K_+}(\mathfrak{l}) = +1,$$

i.e.,  $\mathfrak{l}$  splits in  $K/K_+$ . The first two assertions of Theorem 3 imply the desired assertion.

We prove the third assertion. By Lemma 9-(iv), the prime number  $l$  remains inertia or splits completely in  $K_+/\mathbf{Q}$ . In the former case,

$$\chi_{K/K_+}(l\mathfrak{o}) = \left(\frac{-q'}{l}\right) = +1$$

implies splitting of  $l\mathfrak{o}$  in  $K/K_+$ . Hence, the first three assertions of Theorem 3 imply the desired assertion.

In latter case, we designate by  $\mathfrak{l}_1$ ,  $\mathfrak{l}_2$  and  $\mathfrak{l}_3$  the three prime ideals of  $K_+$  above  $l$ . Then,

$$\chi_{K/K_+}(\mathfrak{l}_1\mathfrak{l}_2\mathfrak{l}_3) = \chi_{K/K_+}(l\mathfrak{o}) = \left(\frac{-q'}{l}\right) = +1$$

implies  $\chi_{K/K_+}(\mathfrak{l}_i) = +1$  for some  $i$ . Hence, the first three assertions of Theorem 3 imply the desired assertion.

The last assertion follows from the first three assertion of the Theorem. **qed.**

## References

- [1] S. Bessassi, “Bounds for the degrees of CM-fields of class number one”, *Acta Arith.* 106 (2003) 213–245.
- [2] G. Bouteaux, “Le problème du nombre de classes 1 pour les corps à multiplication complexe sextiques non galoisiens”, preprint.
- [3] K.-Y. Chang and S.-H. Kwon, “Class numbers of imaginary abelian number fields”, *Proc. Amer. Math. Soc.* 128 (2000) 2517–2528.
- [4] K.-Y. Chang and S.-H. Kwon, “The class number one problem for some non-abelian normal CM-fields of degree 48”, *Math. Comp.* 72 (2003) 1003–1017 (electronic).
- [5] H. Cohen, *Advanced Topics in Computational Number Theory*, GTM 193, Springer-Verlag (2000).
- [6] P. Erdős, “Arithmetical properties of polynomials”, *J. London Math. Soc.* 28 (1953) 416–425.
- [7] H. Hasse, “Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage”, *Math. Z.* 31 (1930) 565–582; *Mathematische Abhandlungen Band 1*, de Gruyter (1975) 423–440.
- [8] S.-H. Kwon and Y.-H. Park, “Determination of all imaginary abelian sextic number fields with class number  $\leq 11$ ”, *Acta Arith.* 82 (1997), 27–43.

- [9] F. Lemmermeyer, “Ideal class groups of cyclotomic number fields I”, *Acta Arith.* 72 (1995) 347–359.
- [10] S. Louboutin and R. Okazaki, “Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one”, *Acta Arith.* 67 (1994) 47–62.
- [11] R. Okazaki “Non-normal class number one problem and the least prime power-residue”, in *Number Theory and its Applications* (S. Kanemitsu and K. Győry eds.) Kluwer Academic Publishers (1999) 273–289.
- [12] R. Okazaki, “Inclusion of CM-fields and divisibility of relative class numbers”, *Acta Arith.* 92 (2000) 319–338.
- [13] R. Okazaki, “On class number one problem in non-normal sextic CM-fields with imaginary quadratic subfields”, preprint.
- [14] I. Schur, “Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten”, *Math. Z.* 1 (1918) 377–402.
- [15] M. Suzuki, *Group Theory vol. I*, Springer Verlag (1982).
- [16] 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.
- [17] K. Uchida, “Imaginary abelian number fields with class number one”, *Tôhoku Math. J. (2)* 24 (1972) 487–499.
- [18] L. C. Washington, *Introduction to Cyclotomic Fields*, GTM 83, Springer (1982) 2nd ed. (1997).
- [19] K. Yamamura, “The determination of the imaginary abelian number fields with class number one”, *Math. Comp.* 62 (1994) 899–921.

Ryotaro OKAZAKI,  
Doshisha University,  
Department of Mathematics,  
Kyotanabe, Kyoto, 610-0394, JAPAN  
email: rokazaki@dd.iij4u.or.jp  
http://www1.doshisha.ac.jp/~rokazaki