ACTA ARITHMETICA
XCII.4 (2000)

Inclusion of CM-fields and divisibility of relative class numbers

by

Ryotaro Okazaki (Kyotanabe)

1. Introduction. In this paper, an algebraic extension of $\mathbb{Q}$ of finite degree is called a *number field*. The class number of a number field F is denoted by h_F. A totally imaginary quadratic extension F of a totally real number field is called a *CM-field*. The maximal totally real subfield of F is denoted by F_+. It is known that h_{F_+} divides h_F. The quotient $h_F^- = h_F/h_{F_+}$ is called the *relative class number* of F. When two CM-fields k and K satisfy $k \subset K$, we say $k \subset K$ are (two) CM-fields.

Horie [12, Theorem 1] showed that $h_k^- \mid 4h_K^-$ for an arbitrary pair of imaginary abelian number fields k and K such that $k \subset K$. We generalize this as follows:

Theorem 1. *Let $k \subset K$ be two CM-fields. Then*

$$h_k^- \mid 4h_K^-. \tag{1}$$

The coefficient 4 is best possible: $h_k^- = 4$ and $h_K^- = 1$ holds for $k = \mathbb{Q}(\sqrt{-3\cdot 4\cdot 7})$ and $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-4}, \sqrt{-7})$. We are not assuming K/k to be normal in Theorem 1. Horie's proof uses decomposition of relative class numbers into generalized Bernoulli numbers via analytic class number formula. Our proof, in contrast, is purely algebraic.

Theorem 3 of [12] determines a necessary and sufficient condition for $h_k^- \nmid 2h_K^-$ under the assumption k and K are imaginary abelian 2-fields. In particular, it is necessary that K contains the class field associated with $\mathcal{C}_k^2$, where $\mathcal{C}_k$ denotes the class group of k. However, it is an open problem whether $h_k^- \nmid 2h_K^-$ necessarily implies that the class field associated with $\mathcal{C}_k^2$ is contained in K in general. It is also open whether $h_k^- \nmid h_K^-$ necessarily implies that K contains a quadratic extension of k. There are examples of pairs of k and K with $h_k^- \nmid h_K^-$ such that K contains a ramified quadratic extension

2000 *Mathematics Subject Classification*: 11R29, 11R37, 11R42.

of k but no unramified quadratic extensions of k (cf. the first remark to Corollary 28).

An obvious application of Theorem 1 is the following:

Corollary 2. *Let k be an imaginary quadratic field contained in a CM-field K whose relative class number is* 1*. Then*

$$h_k = 1, 2 \text{ or } 4. \tag{2}$$

In particular, the number of the prime divisors of the discriminant of k is at most 3.

The second assertion is interesting in connection with class field towers. An imaginary quadratic field with 6 or more prime divisors of discriminant has an infinite 2-class field tower (cf. [20]). The 2-rank of the class group of a field in such a class field tower is greater than 1. Therefore, the relative class number of a CM-field in such a tower is even (cf. the second remark to Lemma 26). Corollary 2 is stronger than such an application of infinite class field tower. (It also states that the 2-class field tower of an arbitrary imaginary quadratic field with four or more prime divisors of discriminant never terminates in the class of CM-fields, i.e., it may terminate but the maximal unramified 2-extension is not a CM-field (cf. [17, pp. 211–212]).

The first assertion of Corollary 2 and determination of all imaginary quadratic fields of class number $1, 2$ and 4 by Heegner [8], Baker [2, 3], Stark [23, 24], Lehmer–Lehmer–Shanks [14], Montgomery–Weinberger [19], Goldfeld [5], Gross–Zagier [6] and Arno [1] imply the following:

Theorem 3. *Let N be a normal CM-field whose relative class number is* 1 *and d_N its discriminant. A zero of the Dedekind zeta function ζ_N of N in the interval $[1 - 2/(3 + 2\sqrt{2})\log|d_N|, 1[$, if any, is a zero of the Dedekind zeta function ζ_F of some real quadratic subfield F of N.*

Remark. Theorem 3 asserts that a possible Siegel's zero of a Dedekind zeta function of a normal CM-field of relative class number one is benign. For example, it suggests a possibility of improving Hoffstein's bound [11] on the degree of (normal) CM-fields of relative class number one.

We shall employ three basically different tools for proving Theorem 1: a class number relation, a field theoretic tool, and a group theoretic tool. The first tool is well known. However, Lemmermeyer's presentation [15] is particularly suitable for our purpose. The second and the third tools will be developed for our purpose. In the development of the field theoretic tool, understanding of CM-fields in terms of Galois theory will be required.

Therefore, we shall review the standard theory of Galois properties of CM-fields in Section 2; quote Lemmermeyer's class number relation and collect the necessary standard facts on indices related with CM-fields in Section 3; develop a field theoretic tool for the study of relative class numbers in Section 4; develop a group theoretic tool for the study of relative class numbers in Section 5; investigate a certain intermediate field of CM-fields in Section 6; and lastly prove the main results in Section 7.

It turns out that the field theoretic tool gives interesting results by itself. Indeed, it reveals an interesting relation of unramifiedness and divisibility of relative class numbers (cf. Propositions 22 and 23). Theorem 30 of Section 6, which is the Key Lemma for our proof of Theorem 1, has more information than Theorem 1. Hence, the object of Theorem 30 is studied in more detail.

The author expresses his gratitude to Professor K. Miyake for helpful discussions.

2. CM-fields. In Section 4, we shall prove surprising statements (Propositions 22 and 23) via class field theory and the theory of CM-fields. The theory of CM-fields will be used in a complicated situation: CM-fields will often appear as subfields of non-CM-fields and often be non-normal; their automorphism groups (instead of Galois groups) will be investigated. For convenience of the readers who check the proofs of Section 4, we review here the standard theory of CM-fields.

We follow [22, Lemma 3 (p. 66)] (cf. also [21, Lemma 18.2 (p. 122)] and [7]). We adopt an alternative definition of a CM-field (Definition 5) which is more convenient than the definition given at the beginning of this paper. Equivalence of the two definitions is verified in Lemma 9. We give several examples for indicating how the standard theory avoids troubles related to the above mentioned situation.

Definition 4. Let F be a number field. Then an automorphism $\sigma \in \mathrm{Aut}(F/\mathbb{Q})$ is called a *complex conjugation* of F if $\sigma\tau = \tau\sigma_{\mathbb{C}}$ for an imaginary embedding τ of F and the complex conjugation $\sigma_{\mathbb{C}}$ of $\mathbb{C}$.

A complex conjugation is necessarily an involution: Let σ be a complex conjugation of F with respect to an imaginary embedding τ. Then $\sigma^2\tau = \sigma\tau\sigma_{\mathbb{C}} = \tau\sigma_{\mathbb{C}}^2 = \tau$. Hence, $\sigma^2 = 1$ since τ is injective. It is obvious from the definition that a complex conjugation is non-trivial.

Example A1. Let $F = \mathbb{Q}(\sqrt{-3-2\sqrt{5}})$. Here $\sqrt{-3-2\sqrt{5}}$ stands for a root α of X^4+6X^2-11, i.e., X in $\mathbb{Q}[X]/(X^4+6X^2-11)$. The field F has two real embeddings and a pair of imaginary embeddings. There is no complex conjugation with respect to either of the two real embeddings. On the other hand, the automorphism induced by $\alpha \mapsto -\alpha$ is a complex conjugation with respect to any of the two imaginary embeddings.

Example A2. Let $F = \mathbb{Q}(\sqrt{2+\sqrt{-3}})$. Here $\sqrt{2+\sqrt{-3}}$ stands for a root α of X^4-4X^2+7, i.e., X in $\mathbb{Q}[X]/(X^4-4X^2+7)$, and $\sqrt{-3}$ stands for α^2-2. If a complex conjugation of F exists, it must carry $\sqrt{-3}$ to $-\sqrt{-3}$ and hence $2+\sqrt{-3}$ to $2-\sqrt{-3}$. However, the former is a square in F but the latter is not. Hence, no automorphism of F can carry $\sqrt{-3}$ to $-\sqrt{-3}$. The contradiction proves that F has no complex conjugation although it is totally imaginary. This example also tells us that a complex conjugation of a subfield does not necessarily extend to a complex conjugation of an extension field.

A complex conjugation with respect to a given imaginary embedding, if any, is unique since τ is injective. (Strictly speaking, we can talk of *the* complex conjugation *with respect to* τ.) In particular, the relation $\sigma\tau = \tau\sigma_{\mathbb{C}}$ uniquely determines a complex conjugation σ with respect to an imaginary embedding τ if the image of τ is closed under $\sigma_{\mathbb{C}}$. This is the case when F is normal and totally imaginary. However, a complex conjugation of a normal totally imaginary number field depends, in general, on the imaginary embedding.

Example A3. Let $F = \mathbb{Q}(\sqrt[6]{-3})$. Then F is normal and totally imaginary. Write $\alpha = \sqrt[6]{-3}$. Then the automorphism ϱ induced by $\alpha^2 \mapsto \alpha^2$ and $\alpha^3 \mapsto -\alpha^3$ is a complex conjugation with respect to an imaginary embedding which maps α^2 to the real cube root of -3.

Conversely, let τ be an imaginary embedding of F such that ϱ is a complex conjugation with respect to τ. Then $\alpha^{2\tau} = \alpha^{2\varrho\tau} = \alpha^{2\tau\sigma_{\mathbb{C}}}$. Hence, $\alpha^{2\tau}$ is real. Therefore, the equality $(\alpha^2)^3 = -3$ implies that $\alpha^{2\tau}$ is necessarily the real cube root of -3.

We saw that ϱ is not a complex conjugation with respect to any imaginary embedding which carries α^2 to an imaginary cube root of -3.

The Galois property of $\mathbb{Q}(\sqrt[6]{-3})$ is similar to that of the class field $\mathbb{Q}(\sqrt{-23})[X]/(X^3-X-1)$ of $\mathbb{Q}(\sqrt{-23})$, which is more related to the topic of this paper.

Definition 5. A totally imaginary number field is called a *CM-field* if a complex conjugation with respect to each imaginary embedding makes sense and is independent of the imaginary embedding.

We can speak of *the* complex conjugation of a CM-field F. (We can say that the complex conjugation of F makes sense if and only if F is a CM-field.) It will be verified later in Lemma 9 that Definition 5 coincides with the ordinary definition of a CM-field quoted at the beginning of this paper.

The complex conjugation of a CM-field has an important property:

Lemma 6. *The complex conjugation σ of a CM-field F commutes with* $\mathrm{Aut}(F/\mathbb{Q})$.

Proof. Let ϱ be an arbitrary element of $\mathrm{Aut}(F/\mathbb{Q})$ and τ an arbitrary imaginary embedding of F. Then σ is a complex conjugation with respect to τ and $\varrho\sigma\varrho^{-1}$ is a complex conjugation with respect to $\varrho\tau$. (Verify $\varrho\sigma\varrho^{-1}\,\varrho\tau = \varrho\sigma\tau = \varrho\tau\sigma_{\mathbb{C}}$.) Independence of σ of the choice of an imaginary embedding implies $\sigma = \varrho\sigma\varrho^{-1}$. ■

A converse (in some sense) of Lemma 6 holds:

Lemma 7. *A normal totally imaginary number field N is a CM-field if a complex conjugation σ of N commutes with* $\mathrm{Gal}(N/\mathbb{Q})$.

Proof. Assume that σ is a complex conjugation with respect to an imaginary embedding τ of N. Then an arbitrary imaginary embedding of N is written as $\varrho\tau$ with some $\varrho \in \mathrm{Gal}(N/\mathbb{Q})$. The commutation relation $\sigma\varrho\tau = \varrho\tau\sigma_{\mathbb{C}}$ follows from $\sigma\tau = \tau\sigma_{\mathbb{C}}$ and the assumption that σ commutes with $\mathrm{Gal}(N/\mathbb{Q})$. ■

Example A4. Normality in Lemma 7 is essential in a certain sense: Some (non-normal) totally imaginary number field F is not a CM-field while it has a complex conjugation which commutes with $\mathrm{Aut}(F/\mathbb{Q})$. An example is $F = \mathbb{Q}[X]/(X^6 - X^2 + 1)$. Denote by $\sqrt{-\beta}$ the residue class of X. Then β is a root of $Y^3 - Y - 1$. It is easily verified, by differentiation, that β has a real embedding and a pair of imaginary embeddings. The image of the unique real embedding of β is positive. Therefore, $\sqrt{-\beta}$ is totally imaginary, i.e., F is totally imaginary. Since the discriminant of $Y^3 - Y - 1$ is -23, the normal closure of $\mathbb{Q}(\beta)$ is $\mathbb{Q}(\beta, \sqrt{-23}\,)$. On the other hand, the norm $N_{\mathbb{Q}(\beta)/\mathbb{Q}}(23\beta) = 23^3$ is not a square in $\mathbb{Q}$. Hence, 23β is not a square in F $(= \mathbb{Q}(\sqrt{-\beta}\,))$. Thus, F does not contain the normal closure of $\mathbb{Q}(\beta)$. (Hence, F is non-normal.) Since β is cubic, this implies that β is a unique root of $Y^3 - Y - 1$ that is contained in F. Therefore, $\mathrm{Aut}(F/\mathbb{Q})$ consists of the identity and the automorphism σ induced by $\sqrt{-\beta} \mapsto -\sqrt{-\beta}$. The non-trivial automorphism σ is a complex conjugation with respect to an embedding of F in which β is mapped to a real number. It obviously commutes with the group $\mathrm{Aut}(F/\mathbb{Q})$ of order 2. However, σ is not a complex conjugation with respect to any embedding of F in which β is mapped to a complex number. Therefore, F is not a CM-field.

For convenience, we introduce the term CM-extension:

Definition 8. A totally imaginary quadratic extension of a totally real number field is called a *CM-extension*.

Definition 5 of a CM-field coincides with the ordinary definition:

Lemma 9. *A number field F is a CM-field if and only if it is a CM-extension of a totally real number field. Further, the maximal totally real subfield F_+ of a CM-field F is identified as the fixed field of the complex conjugation of F.*

Proof. We first assume F to be a CM-field. Let σ denote the complex conjugation of F. Then the fixed field F_0 of σ has a real image under an arbitrary imaginary embedding τ of F. (To see this, verify $\alpha^\tau = \alpha^{\sigma\tau} = \alpha^{\tau\sigma_{\mathbb{C}}}$ for an arbitrary element α of F_0.) Since τ is arbitrary, this implies that F_0 is totally real. Conversely, an arbitrary totally real subfield of F is fixed by σ. (Read the commutation relation of σ from right to left.) Therefore, F_0 is identical to the maximal totally real subfield F_+ of F. Since σ is an involution, F/F_0 is quadratic. Therefore, a CM-field is necessarily a CM-extension of a totally real number field. The "only if" part of the first assertion and the second assertion are proven.

Let F be a CM-extension of a totally real number field M, σ the nontrivial conjugation of F/M and τ an arbitrary imaginary embedding of F. Assume α generates F/M. We can assume $\alpha^\sigma = -\alpha$ by replacing α with $\alpha - \alpha^\sigma$ if necessary. It is obvious that α^2 is invariant under σ, i.e., $\alpha^2 \in M$. Moreover, $(\sigma\tau)|_M = \tau|_M = (\tau\sigma_{\mathbb{C}})|_M$ since σ is trivial on M. In particular, $\alpha^{2\sigma\tau} = \alpha^{2\tau} = \alpha^{2\tau\sigma_{\mathbb{C}}}$. Therefore, $\alpha^{\sigma\tau} = -\alpha^\tau = \alpha^{\tau\sigma_{\mathbb{C}}}$. (Note that $\alpha^\tau \neq \alpha^{\tau\sigma_{\mathbb{C}}}$ since α is totally imaginary.) We get $\sigma\tau = \tau\sigma_{\mathbb{C}}$ since both sides coincide on M and on the generator α of F/M. Since τ is arbitrary, σ is the complex conjugation of F. Thus, F is a CM-field. ∎

Example A5. Let $F = \mathbb{Q}(\sqrt{-9-\sqrt{13}})$. Write $\alpha = \sqrt{-9-\sqrt{13}}$. Then $\alpha \mapsto -\alpha$ induces the complex conjugation of F.

Lemma 10. *The composition of two CM-fields is also a CM-field.*

Proof. Let F_1 and F_2 be two CM-fields. Denote by σ_{F_1} and σ_{F_2} respectively the complex conjugation of F_1 and F_2. Put $F = F_1F_2$ and let L be the normal closure of F. Then F and L are totally imaginary. Let τ_0 be an imaginary embedding of L and σ a complex conjugation of L with respect to τ_0. (Normality of L guarantees the existence of σ.) We have $\sigma|_{F_i}\tau_0 = \tau_0|_{F_i}\sigma_{\mathbb{C}} = \sigma_{F_i}\tau_0|_{F_i}$ for $i = 1, 2$. Noting that τ_0 is injective, we get $\sigma|_{F_i} = \sigma_{F_i}$. Hence, $\sigma|_F$ induces the unique automorphism $\sigma_F \in \mathrm{Aut}(F/\mathbb{Q})$ that induces σ_{F_i} on F_i for $i = 1, 2$. (Note that $\sigma|_F$ preserves F_1 and F_2 so that $\sigma|_F$ preserves $F = F_1F_2$.)

Let τ be an arbitrary imaginary embedding of L. Then the conclusion of the previous paragraph implies $\sigma|_{F_i}\tau = \sigma_{F_i}\tau|_{F_i} = \tau|_{F_i}\sigma_{\mathbb{C}}$ for $i = 1, 2$. Since $F = F_1F_2$, this implies $\sigma_F\tau|_F = \sigma|_F\tau = \tau|_F\sigma_{\mathbb{C}}$. Since an arbitrary imaginary embedding of F is obtained by restricting an imaginary embedding of L, this identity and Definition 5 imply that F is a CM-field. ∎

Lemma 11. *The normal closure of a CM-field is also a CM-field.*

Proof. Let F be a CM-field. Then all conjugate fields of F are CM-fields. By Lemma 10, the composition of all conjugate fields of F is a CM-field. ■

A CM-field has a nice property with respect to subfields:

Lemma 12. *A subfield of a CM-field is either a CM-field or a totally real number field. In particular, an intermediate field of two CM-fields is a CM-field.*

Let k be a subfield of a CM-field K and assume k not to be totally real. Let N be the normal closure of K. Then N is a CM-field by Lemma 11. Let σ denote the complex conjugation of N. Since k is not totally real, $\sigma \notin \mathrm{Gal}(N/k)$. Since σ commutes with $\mathrm{Gal}(N/\mathbb{Q})$ by Lemma 7, σ normalizes $\mathrm{Gal}(N/k)$. Therefore, σ acts non-trivially on k, i.e., $\sigma|_k$ induces $\sigma_k \in \mathrm{Aut}(k/\mathbb{Q}) - \{1\}$. The commutation relation $\sigma_k\tau = \tau\sigma_{\mathbb{C}}$ for an arbitrary archimedean embedding τ of k follows from the corresponding relation for σ. Since σ_k is non-trivial and τ is injective, the embeddings $\tau\sigma_{\mathbb{C}} = \sigma_k\tau$ and τ are different. Hence, an arbitrary archimedean embedding τ is necessarily imaginary, i.e., k is totally imaginary. Now, the field k satisfies the conditions of Definition 5 and hence is a CM-field. ■

Remark. Lemma 12 holds in the following sense: if $k \subset K$ are two CM-fields, the restriction to k of the complex conjugation K is the complex conjugation of k.

Remark. Lemmata 11 and 12 imply the following equivalence: a number field is a CM-field if and only if its normal closure is a CM-field.

3. Units and class groups. In this section, we collect basic definitions and facts concerning indices related with CM-fields. We also quote a property of a class group and Lemmermeyer's class number relation.

We write respectively $\mathcal{C}_F$ and $\mathcal{C}_F^+$ for the (weak) class group and the strict class group of a number field F. We call $h_F = \#\mathcal{C}_F$ the (weak) class number of F and $h_F^+ = \#\mathcal{C}_F^+$ the strict class number of F. We write respectively E_F and E_F^+ for the unit group and the totally positive unit group of F. We denote by W_F the group of roots of unity of F and by w_F its order.

Let F be a CM-field. We write F_+ for the maximal totally real subfield of F; h_F^- for the relative class number h_F/h_{F_+}; and ι_F for the natural map from the group of ideals of F_+ to F. The subscript F is omitted if it is obvious. The order of the kernel of the homomorphism $\mathcal{C}_{F_+} \to \mathcal{C}_F$ induced by ι_F is denoted by κ_F. The Hasse unit index $[E_F : W_F E_{F_+}]$ is denoted by Q_F.

Note that the plus sign in $\mathcal{C}_F^+$ designates "strict sense" here while it designates "relation with the maximal totally real subfield" in many positions of the literature.

DEFINITION 13. A CM-field F is said to be of *unit radical form* if $F = F_+(\sqrt{-\eta})$ for some $\eta \in E_{F_+}^+$. A CM-field F is said to be *non-primary* if $F = F_+(\sqrt{-\delta})$ for some $\delta \in F_+$ which generates a square ideal of F_+; it is said to be *primary* otherwise.

LEMMA 14. *Let F be a CM-field. Then $\kappa_F Q_F \mid 2$. When $\kappa_F Q_F = 2$, the CM-field F is non-primary. When $Q_F = 2$, the CM-field F is of unit radical form. Conversely, a non-primary CM-field F satisfies $\kappa_F Q_F = 2$ unless $F = F_+(\sqrt{-1})$. A CM-field F of unit radical form satisfies $Q_F = 2$ unless $F = F_+(\sqrt{-1})$. Moreover, F is non-primary if F/F_+ is unramified at the finite primes. On the other hand, F/F_+ is unramified at all odd primes if F is non-primary.*

Proof. This is well known (cf. [16] or [27, Theorems 4.12 and 10.3]). ■

LEMMA 15. *Let M be a totally real number field and r the 2-rank of $\mathcal{C}_M^+$. Then the number of non-primary CM-extensions F/M is 2^r. Hence, the number of CM-extensions F/M such that $\kappa_F Q_F = 2$ is either $2^r - 1$ or 2^r. Moreover, there is no CM-extension F/M such that $\kappa_F Q_F = 2$ if $r = 0$.*

Proof. Let C_1 be the group of strict ideal classes which are principal in the weak sense and C_2 the group of strict ideal classes whose squares are principal in the strict sense. Set $m = \#(C_2/C_1)$ and let ideals $\mathfrak{d}_i$ with $i \in \{1, \ldots, m\}$ be a complete system of representatives for C_2/C_1. Choose a totally positive generator $\delta_i \in M$ of $\mathfrak{d}_i^2$ for each $i = 1, \ldots, m$. Let η_j with $j \in \{1, \ldots, n = \#C_1\}$ be a complete system of representatives for E_F^+/E_F^2. Then each $M(\sqrt{-\delta_i\eta_j})$ with $i = 1, \ldots, m$ and $j = 1, \ldots, n$ is a non-primary CM-extension of M. Conversely, any non-primary CM-extension F of M is of the above form. The first assertion is now obvious. By Lemma 14, we get the second assertion. Assume $r = 0$ and let F be an arbitrary CM-extension of M. Then $\kappa_F = 1$ follows from the first assertion of Lemma 14. The fact $Q_F = 1$ is well known (cf. [16]). ■

EXAMPLE B1. Let $F_+ = \mathbb{Q}(\sqrt{12})$ with $F = F_+(\sqrt{-4})$ or $F_+(\sqrt{-8})$. Then $Q_F = 2$. The extension F/F_+ is unramified at the finite primes in the former case, and is ramified above (2) in the latter.

EXAMPLE B2. Let $F_+ = \mathbb{Q}(\sqrt{40})$ with $F = F_+(\sqrt{-4})$ or $F_+(\sqrt{-8})$. Then $\kappa_F = 2$. The extension F/F_+ is ramified above (2).

EXAMPLE B3. Let $F_+ = \mathbb{Q}(\sqrt{60})$ with $F = F_+(\sqrt{-3}), F_+(\sqrt{-4})$, $F_+(\sqrt{-8})$ or $F_+(\sqrt{-24})$. Then $Q_F = 2$ and $\kappa_F = 1$ in the last case, and $Q_F = 1$ and $\kappa_F = 2$ in the other cases. The extension F/F_+ is unramified at the finite primes in the former two cases, and ramified above (2) in the latter two cases.

Example B4. Let $F_+ = \mathbb{Q}(\sqrt{5})$ with $F = F_+(\sqrt{-4})$. Then $\kappa_F = Q_F = 1$. The extension F/F_+ is ramified above (2).

Lemma 16. *Let $k \subset K$ be two CM-fields. Then $\kappa_k\, Q_k w_k \mid \kappa_K\, Q_K w_K$ and $Q_k w_k \mid Q_K w_K$. In particular, $\kappa_k = \kappa_K$ and $Q_k = Q_K$ if $[K : k]$ is odd.*

Proof. This follows from a characterization of κ_F and Q_F of a CM-field F that is used in the proofs for [27, Theorems 4.12 and 10.3] (cf. [10] for subtle examples). ■

Lemma 17. *Let F be a CM-field and t the number of finite primes of F_+ ramified in F/F_+. Assume that the 2-rank of $\mathcal{C}^+_{F_+}$ is zero. Then the 2-rank of $\mathcal{C}_F$ is $t-1$.*

Proof. This is well known: it is summarized in Satz 15 of Takagi's fundamental paper [26, p. 106] on class field theory; notation and terminology defined in Satz 14 of p. 103 and the second footnote of p. 100 of the cited paper. The proofs of Satz 14 and Satz 15 also prove the lemma.

For convenience of the reader, the following argument recovers the lemma from the assertion of Satz 15.

An ideal class of a CM-field F is called *ambiguous* if the complex conjugation of F fixes it. Let $\mathcal{A}_F$ be the group of ambiguous ideal classes of F. Let $\widetilde{Q}_F$ be the index of $E^2_{F_+}$ in $N_{F/F_+}F^\times \cap E_{F_+}$. Satz 15 evaluates the order of $\mathcal{A}_F$:

$$\#\mathcal{A}_F = \frac{\widetilde{Q}_F}{Q_F}\, 2^{t-1} h_{F_+}.$$

In the situation of the lemma, the quotient of indices is 1.

On the other hand, the group $\mathcal{A}_F$ is isomorphic to the direct product of $\iota\mathcal{C}_{F_+}$ and $\ker(2 : \mathcal{C}_F \to \mathcal{C}_F)$. Here, the group $\iota\mathcal{C}_{F_+}$ is isomorphic to $\mathcal{C}_{F_+}$ since h_{F_+} is odd and κ_F divides 2 by Lemma 14. The formula of the previous paragraph and the isomorphisms imply the lemma. ■

We quote Lemmermeyer's class number relation from [15].

Lemma 18. *Let L_1 and L_2 be two distinct CM-extensions of L_+ and $M = L_1L_2$. Then*

$$h^-_M = \frac{[E_M : E_{M_+}E_{L_1}E_{L_2}]}{2^{1+v}} h^-_{L_1} h^-_{L_2} \tag{3}$$

where $v = 1$ if both L_1 and L_2 are of unit radical form, and $v = 0$ otherwise.

This relation agrees with the analytic class number formula (cf. [16]). This presentation is more convenient for our purpose. It also enables us to algebraically prove everything but Theorem 3 since it has a purely algebraic proof (cf. [15]).

4. Maximal CM-fields in class fields. Many facts concerning relative class numbers of CM-fields are found via field theoretic arguments on subfields of class fields.

Let F be a number field. We denote by $\mathcal{H}_F$ the Hilbert class field of F, i.e., the maximal unramified abelian extension of F. Assume F to be a CM-field. We have $h_F^- = [\mathcal{H}_F : F\mathcal{H}_{F_+}]$ by class field theory.

Definition 19. Let F be a CM-field. Then $\mathcal{H}_F^0$ denotes the maximal CM-field in the Hilbert class field $\mathcal{H}_F$ of F.

This definition makes sense since F is a CM-field and the class of CM-fields is closed under composition by Lemma 10. The following two properties of $\mathcal{H}_F^0/F_+$ are essential.

Lemma 20. *Let F be a CM-field. Then $\mathcal{H}_F^0/F_+$ is abelian.*

Proof. By definition, $\mathcal{H}_F^0/F$ is abelian. Hence, $\mathrm{Aut}(\mathcal{H}_F^0/F_+)$ contains an abelian subgroup $\mathrm{Gal}(\mathcal{H}_F^0/F)$. Let σ be the complex conjugation of $\mathcal{H}_F^0$. It acts trivially on the maximal totally real subfield of $\mathcal{H}_F^0$. Hence, it fixes F_+, i.e., $\mathrm{Aut}(\mathcal{H}_F^0/F_+)$ contains σ. By Lemma 6, σ commutes with $\mathrm{Aut}(\mathcal{H}_F^0/F_+)$. Hence, the group G generated by σ and $\mathrm{Gal}(\mathcal{H}_F^0/F)$ is abelian.

Since σ acts non-trivially on F, the order of G is larger than $\mathrm{Gal}(\mathcal{H}_F^0/F)$. Hence, the fixed field of G is a proper subfield of F. Since G fixes F_+ and F/F_+ is quadratic, the fixed field of G coincides with F_+. Therefore, $\mathcal{H}_F^0/F_+$ is normal and $\mathrm{Gal}(\mathcal{H}_F^0/F_+) = G$. Since G is abelian, the assertion follows. ∎

Lemma 21. *Let $k \subset K$ be two CM-fields. Then $[\mathcal{H}_k : \mathcal{H}_k^0] \mid h_K^-$.*

Proof. Let $H = K\mathcal{H}_{K_+} \cap \mathcal{H}_k$. Then $[\mathcal{H}_k : H] = [K\mathcal{H}_{K_+}\mathcal{H}_k : K\mathcal{H}_{K_+}]$ since $\mathcal{H}_k/k$ is normal. Since $K\mathcal{H}_{K_+} \subset K\mathcal{H}_{K_+}\mathcal{H}_k \subset \mathcal{H}_K$, $[K\mathcal{H}_{K_+}\mathcal{H}_k : K\mathcal{H}_{K_+}]$ divides $h_K^- = [\mathcal{H}_K : K\mathcal{H}_{K_+}]$. On the other hand, H is an intermediate field between the CM-fields k and $K\mathcal{H}_{K_+}$. Hence, H is a CM-field by Lemma 12. Since it is a subfield of $\mathcal{H}_k$, it follows that $H \subset \mathcal{H}_k^0$. Therefore, $[\mathcal{H}_k : \mathcal{H}_k^0]$ divides $[\mathcal{H}_k : H]$. The lemma follows immediately from the identity and the two divisibility relations. ∎

Lemma 21 is a nice tool for the study of relations between relative class numbers. An application is the following:

Proposition 22. *Let $k \subset K$ be two CM-fields and assume k/k_+ is unramified at the finite primes. Then $h_k^- \mid h_K^-$.*

Proof. Let $H = \mathcal{H}_k^0$. Then H/k_+ is abelian by Lemma 20 and so is H_+/k_+. Since k/k_+ is unramified at the finite primes, so is H/k_+. Hence, H_+/k_+ is an unramified abelian extension, i.e., $H_+ \subset \mathcal{H}_{k_+}$. The converse

$\mathcal{H}_{k_+} \subset H_+$ is obvious. Therefore, we get the identity $H_+ = \mathcal{H}_{k_+}$. Since $k \subset H$, we have $kH_+ \subset H$. Comparison of degrees over H_+ implies the identity $kH_+ = H$. These two identities and the choice of H imply $k\mathcal{H}_{k_+} = \mathcal{H}_k^0$. Hence, $h_k^- = [\mathcal{H}_k : \mathcal{H}_k^0]$. Now, Lemma 21 implies the desired assertion. ■

Although Proposition 22 is not used in our proof for Theorem 1, it is interesting in its own right since it illustrates that something stronger than Theorem 1 can be said in an interesting situation.

The method for proving Lemma 21 also gives the following:

PROPOSITION 23. *Let $k \subset K$ be two CM-fields and assume K_+/k_+ is unramified. Then $h_k^- \mid h_K^-$.*

Proof. Let $H = K\mathcal{H}_{K_+} \cap \mathcal{H}_k$. Then $H \subset \mathcal{H}_k^0$ by Lemma 12. Hence, H_+/k_+ is abelian by Lemma 20. On the other hand, $H_+ \subset (K\mathcal{H}_{K_+})_+ = \mathcal{H}_{K_+}$ by the choice of H. Since K_+/k_+ is unramified, this implies that H_+/k_+ is unramified. Therefore, $H_+ \subset \mathcal{H}_{k_+}$ and hence $H \subset k\mathcal{H}_{k_+}$. The reverse inclusion is obvious from the choice of H and hence the identity $H = k\mathcal{H}_{k_+}$ follows. Further, the choice of H and normality of $\mathcal{H}_k/H$ imply $[\mathcal{H}_k : H] = [K\mathcal{H}_{K_+}\mathcal{H}_k : K\mathcal{H}_{K_+}] \mid [\mathcal{H}_K : K\mathcal{H}_{K_+}]$. The desired assertion follows from the identity and the divisibility relation. ■

EXAMPLE C1. Let $k = \mathbb{Q}(\sqrt{-31}, \sqrt{-8 \cdot 5})$ and $K = k(\sqrt{5})$. Then k/k_+ is unramified at the finite primes and K_+/k_+ is unramified. We have $h_k^- = 6 \mid h_K^- = 6$.

EXAMPLE C2. Let $k = \mathbb{Q}(\sqrt{-31}, \sqrt{-8 \cdot 5})$ and $K = k(\sqrt{8})$. Then k/k_+ is unramified at the finite primes and K_+/k_+ is ramified at the finite prime above (2). We have $h_k^- = 6 \mid h_K^- = 24$.

EXAMPLE C3. Let $k = \mathbb{Q}(\sqrt{-3}, \sqrt{8 \cdot 5})$ and $K = k(\sqrt{8})$. Then k/k_+ is ramified above the two finite primes above (3) and K_+/k_+ is unramified. We have $h_k^- = 2 \mid h_K^- = 2$.

However, neither unramifiedness of K/K_+ at the finite primes nor unramifiedness of K/k implies $h_k^- \mid h_K^-$:

EXAMPLE C4. Let $k = \mathbb{Q}(\sqrt{-3 \cdot 5}, \sqrt{-7 \cdot 5})$ and $K = k(\sqrt{5})$. Then K/K_+ is unramified at the finite primes and K/k is unramified. However, $h_k^- = 2 \nmid h_K^- = 1$.

LEMMA 24. *Let $k \subset K$ be two CM-fields, and r_1 the 2-rank of* $\ker(N : \mathcal{C}_k \to \mathcal{C}_{k_+})$. *Then $h_k^- \mid 2^{r_1} h_K^-$.*

Proof. Let σ be the complex conjugation of k. By class field theory, $\mathrm{Gal}(\mathcal{H}_k^0/k\mathcal{H}_{k_+})$ is isomorphic as a σ-module to some quotient C_1/C_0 with some subgroup C_0 of the specified kernel which is denoted by C_1. By Lemma 6, the action of σ on $\mathrm{Gal}(\mathcal{H}_k^0/k)$ is trivial and so is its action on

C_1/C_0 by class field theory. By definition of C_1, σ acts as inversion on C_1/C_0. For these two descriptions of σ to agree, we must have $C_1/C_0 \simeq (\mathbb{Z}/2\mathbb{Z})^{r'}$ with some integer $0 \le r' \le r_1$. Hence, we get $[\mathcal{H}_k : \mathcal{H}_k^0] = h_k^-/2^{r'}$. By Lemma 21, we now see that $h_k^-/2^{r'}$ divides h_K^-. The desired assertion follows immediately. ∎

LEMMA 25. *Let $k \subset K$ be two CM-fields and assume $h_K^- = 1$. Then the complex conjugation of k fixes $\mathcal{C}_k$.*

Proof. By Lemma 21, we get $\mathcal{H}_k = \mathcal{H}_k^0$. Hence, by Lemma 6, the action of the complex conjugation σ of k on $\mathrm{Gal}(\mathcal{H}_k/k)$ is trivial. So is the action of σ on $\mathcal{C}_k$ by class field theory. ∎

REMARK. We say a class group $\mathcal{C}_F$ of a CM-field F is *ambiguous* if the complex conjugation of F fixes $\mathcal{C}_F$. Ambiguity of a class group is not inherited by subfields. Let $k = \mathbb{Q}(\sqrt{-7\cdot 8})$ and $K = \mathbb{Q}(\sqrt{-7}, \sqrt{8})$. Then $\mathcal{C}_k \simeq \mathbb{Z}/4\mathbb{Z}$ and $\mathcal{C}_K \simeq \mathbb{Z}/2\mathbb{Z}$. Since the complex conjugation inverts $\mathcal{C}_k$, the class group $\mathcal{C}_k$ ($\simeq \mathbb{Z}/4\mathbb{Z}$) is not ambiguous. On the other hand, $\mathcal{C}_K$ is ambiguous since the automorphism group of $\mathcal{C}_K$ ($\simeq \mathbb{Z}/2\mathbb{Z}$) is 1.

5. Quotients of class groups.

Although many facts are proven via field theoretic arguments, several important facts concerning relative class numbers of CM-fields are proven via group theoretic arguments on class groups. The most natural object related to relative class numbers is the kernel of the norm map of class groups. Surprisingly, however, quotients of ideal groups by liftings of ideals from subfields turn out very useful for our purpose. Hence, we devote a separate section to the discussion of quotients of the form $\mathcal{C}_F/\iota\mathcal{C}_{F_+}$.

It is obvious that

$$h_F^- = \#(\mathcal{C}_F/\iota\mathcal{C}_{F_+})/\,\kappa_F\,. \tag{4}$$

LEMMA 26. *Let F be a CM-field and r be the 2-rank of $\mathcal{C}_{F_+}^+$. Put $u_F = 2$ if F/F_+ is unramified at the finite primes, and $u_F = 1$ otherwise. Then $2^r/u_F\,\kappa_F \mid h_F^-$.*

REMARK. This is a partial refinement of [4, Theorem 2] and [27, Proposition 10.12]. The latter is recovered as follows: When $u_F = 2$, the 2-rank r' of $\mathcal{C}_F$ is less than r. (Note that $2^{r'}$ [resp. 2^r] is the degree (over F_+) of the maximal elementary abelian 2-extension of F_+ that is unramified [resp. unramified at the finite primes].) Hence, the lemma implies $2^{r'}/\kappa_F \mid h_F^-$.

Proof (of Lemma 26). The norm from ideals of F to ideals of F_+ induces a homomorphism $N : \mathcal{C}_F \to \mathcal{C}_{F_+}^+$. (Note that all norms of numbers of F are totally positive.) Obviously, $N(\iota\mathcal{C}_{F_+}^+) = (\mathcal{C}_{F_+}^+)^2$. On the other hand, the index of the image of N in $\mathcal{C}_{F_+}^+$ is u_F, i.e., $\#(N(\mathcal{C}_F)/(\mathcal{C}_{F_+}^+)^2) = 2^r/u_F$. Therefore, $2^r/u_F$ divides $\#(\mathcal{C}_F/\iota\mathcal{C}_{F_+})$. Now, (4) implies the desired assertion. ∎

Remark. Let F be a CM-field of odd relative class number. It is known that the 2-rank of $\mathcal{C}_F$ is at most 1 (cf. [13, Theorem 1]). This assertion is confirmed by Lemma 26: Observe that Lemma 26 or a weaker version [27, Proposition 10.12] implies that the 2-rank of $\mathcal{C}_{F_+}$ is at most 1. Since the 2-parts of $\mathcal{C}_{F_+}$ and $\mathcal{C}_F$ are isomorphic when h_F^- is odd, we conclude that the 2-rank of $\mathcal{C}_F$ is at most 1.

Example D1. In the first case of Example B1, we have $r = 1$, $u_F = 2$, $\kappa_F = 1$ and $h_F^- = 1$. In the latter case, $r = 1$, $u_F = \kappa_F = 1$ and $h_F^- = 2$.

Example D2. In both cases of Example B2, we have $r = 1$, $u_F = 1$, $\kappa_F = 2$ and $h_F^- = 1$.

Example D3. In the former two cases of Example B3, we have $r = 2$, $u_F = \kappa_F = 2$ and $h_F^- = 1$. We have $r = 2$, $u_F = 1$, $\kappa_F = 2$ and $h_F^- = 2$ in the third case, and $r = 2$, $u_F = 1 = \kappa_F = 1$ and $h_F^- = 4$ in the last case. Note that the 2-rank of $\mathcal{C}_F$ and that of E_F^+/E_F^2 equal 1.

Example D4. In Example B4, we have $r = 0$, $u_F = \kappa_F = 1$ and $h_F^- = 1$.

Proposition 27. *Let $k \subset K$ be two CM-fields. Then the exponent of* $\operatorname{coker}(N : \mathcal{C}_K/\iota\mathcal{C}_{K_+} \to \mathcal{C}_k/\iota\mathcal{C}_{k_+})$ *divides* 2.

Proof. Let $C = \operatorname{Im}(N : \mathcal{C}_K \to \mathcal{C}_k)\iota\mathcal{C}_{k_+}$. Then, by class field theory, the class field H associated with C is contained in K. Let σ be the complex conjugation of K. Then σ preserves $\mathcal{C}_K$ and hence it preserves $\operatorname{Im}(N : \mathcal{C}_K \to \mathcal{C}_k)$. It obviously preserves $\iota\mathcal{C}_{k_+}$. Therefore, it preserves C. Noting also that σ acts on a field K which contains H, we get an isomorphism $\operatorname{Gal}(H/k) \simeq \mathcal{C}_k/C$ of σ-modules by class field theory.

By Lemma 12, an intermediate field H of K/k is a CM-field. By Lemma 6, the action of σ on $\operatorname{Gal}(H/k)$ is trivial and so is the action of σ on $\mathcal{C}_k/C$. On the other hand, σ acts as inversion on $\mathcal{C}_k/\iota\mathcal{C}_{k_+}$ and hence on $\mathcal{C}_k/C$. Since the two descriptions of the action of σ on $\mathcal{C}_k/C$ agree, the exponent of $\mathcal{C}_k/C$ divides 2. This quotient is the cokernel in question. ∎

Corollary 28. *Let $k \subset K$ be two CM-fields. Assume that K contains at most one quadratic extension of k. Then $h_k^- \mid 4h_K^-$. Assume further that $\kappa_K \mid \kappa_k$. Then $h_k^- \mid 2h_K^-$.*

Proof. Let r be the 2-rank of the cokernel in Proposition 27. Then $\#(\mathcal{C}_k/\iota\mathcal{C}_{k_+})/2^r$ divides $\#(\mathcal{C}_K/\iota\mathcal{C}_{K_+})$ by (4), i.e., h_k^- divides $2^r h_K^- \kappa_K / \kappa_k$. The assumption of the lemma implies $r \le 1$ by class field theory. The desired assertions follow immediately from Lemma 14. ∎

REMARK. There are examples of $h_k^- \nmid h_K^-$ with $N : \mathcal{C}_K \to \mathcal{C}_k$ being surjective: $K = \mathbb{Q}(\sqrt{-8}, \sqrt{40})$ and $k = \mathbb{Q}(\sqrt{-20})$ (where K is an F of Example B2/D2); or $K = \mathbb{Q}(\sqrt{-3}, \sqrt{60})$ and $k = \mathbb{Q}(\sqrt{-20})$ (where K is an F of Example B3/D3). On the other hand, there is an example such that $h_k^- \nmid h_K^-$ with $N : \mathcal{C}_K \to \mathcal{C}_k$ not being surjective: $K = \mathbb{Q}(\sqrt{-4}, \sqrt{5})$ and $k = \mathbb{Q}(\sqrt{-20})$ (where K is an F of Example B4/D4).

REMARK. Although calculation of κ_K is difficult in general, Corollary 28 sometimes gives a sharper estimate than Lemma 21.

EXAMPLE E1. Let $p_0 \equiv 3 \pmod 4$ and $p_1 \equiv \ldots \equiv p_r \equiv 1 \pmod 4$ ($r \geq 3$) be distinct prime numbers. Set $k = \mathbb{Q}(\sqrt{-p_0 p_1 \ldots p_r})$ and $K = \mathbb{Q}(\sqrt{-p_0}, \sqrt{p_1 p_2 \ldots p_r})$. Then Corollary 28 yields that $h_k^- \mid 4h_K^-$ while Lemma 21 only gives $h_k^- \mid 2^r h_K^-$.

EXAMPLE E2. Let $k = \mathbb{Q}(\sqrt{-11 \cdot 13 \cdot 29})$ and $K = k[X]/(X^4 - 388X^2 - 3016X - 6096)$. Then $K_+ = \mathbb{Q}[X]/(X^4 - 388X^2 - 3016X - 6096)$ under the obvious inclusion. Calculation with Pari-GP gives the class numbers $h_k = 2^2 \cdot 3$, $h_K = 2^5 \cdot 3 \cdot 13$ and $h_{K_+} = 2^2$. Hence, $h_K^-/h_k^- = (2^3 \cdot 3 \cdot 13)/(2^2 \cdot 3) = 2 \cdot 13 \in \mathbb{Z}$. Calculation with Pari-GP also gives the discriminants $d_{K_+} = 7^2 \cdot 13^2 \cdot 29^2$ and $d_K = 7^4 \cdot 11^4 \cdot 13^4 \cdot 29^4$. From these values of the discriminants, we see $K_+(\sqrt{13}, \sqrt{29})/K_+$ is unramified. Hence, Lemma 21 only explains $3 = h_k^-/4 \mid h_K^-$. However, Proposition 27 explains $h_k^- \mid h_K^-$ as follows: Since an odd prime is ramified in K/K_+, Lemma 14 implies that K is primary. It further implies $\kappa_K = 1$. On the other hand, K_+ is a primitive quartic field whose normal closure has Galois group isomorphic to the alternating group of degree 4. Hence, K_+ does not contain a quadratic extension of $\mathbb{Q}$. Thus, K does not contain a quadratic extension of k. Therefore, the second assertion of Corollary 28 implies $12 = h_k^- \mid h_K^-$.

We also get the following:

COROLLARY 29. *Let $k \subset K$ be two CM-fields. Assume that $[K : k]$ is odd. Then $h_k^- \mid h_K^-$.*

Proof. This is a slight generalization of Proposition 4 of [12]. Here we give a completely different proof, which is independent of normality of K/k.

Since $[K : k]$ is odd, $N : \mathcal{C}_K/\iota\mathcal{C}_{K_+} \to \mathcal{C}_k/\iota\mathcal{C}_{k_+}$ is surjective by Proposition 27 and class field theory. On the other hand, $\kappa_k = \kappa_K$ by Lemma 16. Thus, we get the assertion by (4).

6. An intermediate field. To prove Theorem 1, we shall look at a maximal intermediate field L of K/k such that $h_k^- \mid h_L^-$. Such an intermediate field contains the essential information for our purpose. We describe it in the following:

Theorem 30. *Let $k \subset K$ be two CM-fields and L a maximal intermediate field of K/k (with respect to the partial order "$\subset$") such that $h_k^- \mid h_L^-$. Assume that K contains at least two distinct quadratic extensions of L. Then L satisfies the following conditions*:

(i) *The strict class number $h_{L_+}^+$ is odd.*

(ii) *The number of finite primes ramified in L/L_+ is* 3.

(iii) *The* 2*-rank of $\mathcal{C}_L$ is* 2.

The field K contains three distinct CM-extensions L_1, L_2 and L_3 of L_+ other than L. Each of them satisfies the following conditions:

(iv) *Each extension L_i/L_+ is ramified at a unique finite prime.*

(v) *Each relative class number $h_{L_i}^-$ is odd.*

The CM-extensions, *in combination*, *satisfy the following conditions*:

(vi) *The extensions L_1/L_+, L_2/L_+ and L_3/L_+ are ramified at distinct finite primes.*

(vii) $L \subset L_1L_2L_3$.

(viii) $\mathrm{Im}(N : \mathcal{C}_{LL_1L_2L_3} \to \mathcal{C}_L) = \mathcal{C}_L^2$.

(ix) *The CM-extensions L, L_1, L_2 and L_3 of L_+ are all the CM-extensions of L_+ that are contained in K.*

Proof. Assume that K contains at least two distinct quadratic extensions of L. Then it contains a bicyclic biquadratic extension of L. Hence, K contains at least three quadratic extensions of L.

Let M be a quadratic extension of L in K. Then M is also a CM-field by Lemma 12. Hence, M_+ makes sense and it contains L_+ (cf. Lemma 9). Since M/L_+ is quartic and M/M_+ is quadratic, the extension M_+/L_+ is quadratic. Hence, $M = M_+L$ is bicyclic biquadratic over L_+. Let M_-/L_+ be the other quadratic extension in M/L. Then $M = M_-M_+$ and hence M_- is totally imaginary. By Lemma 9, M_- is a CM-field. We also have $M = M_-L$. It is clear that the correspondence $M \leftrightarrow M_-$ is one-to-one.

Hence, K contains three or more distinct CM-extensions of L_+ other than L. Let $L_1, L_2, L_3, \ldots, L_m$ be the list of such CM-extensions. (Of course, we have $m \geq 3$.) Without loss of generality, we assume that L_1, L_2, L_3 lie in a bicyclic biquadratic extension of L:

Choice. $L \subset L_1L_2L_3$.

We shall prove several claims in order to show the theorem.

Claim 1. *We have $4 \nmid h_{L_i}^-$ for each $i = 1, \ldots, m$ in general and $2 \nmid h_{L_i}^-$ for each $i = 1, \ldots, m$ if L is not of unit radical form. Moreover*, *we have $2 \nmid h_{L_i}^-$ for each $i \in \{1, \ldots, m\}$ such that L_i is not of unit radical form.*

Suppose one of the conditions fails to hold. Then h_L^- would divide $h_{LL_i}^-$ by Lemma 18. This contradicts the maximality of L.

Claim 2. *Two of L_i/L_+'s, say L_2 and L_3, are ramified at some finite prime.*

Suppose, on the contrary, that two of the L_i's, say L_1 and L_2, are unramified extensions of L_+ at the finite primes. Set $M = L_1L_2$. Then M_+/L_+ would be an unramified quadratic extension. Hence, h_L^- must divide h_M^- by Proposition 23. This contradicts the maximality of L since K contains $M = L_1L_2$.

Claim 3. *The 2-rank of $\mathcal{C}_{L_+}^+$ is at most 1.*

Suppose that the 2-rank were greater than 1. One of L_2 or L_3, say L_3, of Claim 2 differs from $L_+(\sqrt{-1})$. By Claim 2, L_3/L_+ is ramified at some finite prime. If L_3 were of unit radical form, we would have $Q_{L_3} = 2$ and hence $\kappa_{L_3} = 1$ by Lemma 14. Then Lemma 26 would imply $4 \mid h_{L_3}^-$. This contradicts Claim 1. If L_3 is not of unit radical form, Lemma 26 would imply $2 \mid h_{L_3}^-$. However, this also contradicts Claim 1.

Claim 4. *The strict class number $h_{L_+}^+$ is odd.*

Suppose it were even. By Lemma 15 and Claim 3, there would be at most two non-primary CM-extensions of L_+. Hence, one of the L_i's, say L_3, would be primary. By Lemma 14, $\kappa_{L_3} = 1$ would hold and L_3/L_+ would be ramified at some finite prime. These and Lemma 26 would imply that $h_{L_3}^-$ should be even. Since L_3 is primary, it cannot be of unit radical form. We got a contradiction to Claim 1.

Claim 5. *Each of $h_{L_1}^-, \ldots, h_{L_m}^-$ is odd.*

Since $h_{L_+}^+$ is odd, $L(\sqrt{-1})$ is the only CM-extension of L_+ of unit radical form by Lemma 15. Hence, either L is not of unit radical form or none of $h_{L_1}^-, \ldots, h_{L_m}^-$ is of unit radical form. Now Claim 1 implies the desired claim.

Claim 6. *Each of $L_1/L_+, \ldots, L_m/L_+$ is ramified at exactly one finite prime.*

Claim 4 implies that each of $L_1/L_+, \ldots, L_m/L_+$ is ramified at some finite prime. Uniqueness follows from Lemma 17, Claims 4 and 5.

Claim 7. *The CM-extensions $L_1/L_+, \ldots, L_m/L_+$ are ramified at distinct finite primes.*

Let χ_i be the character associated with L_i/L_+. Denote by $\mathfrak{f}(\phi)$ the conductor of an ideal character ϕ of L_+. (The conductor is understood to be an ideal, i.e., the "divisor" at infinity is neglected.) For each $i = 1, \ldots, m$, set $\mathfrak{p}_i$ to be the finite prime dividing $\mathfrak{f}(\chi_i)$. (By Claim 6, $\mathfrak{p}_i$ is well defined.)

Let i and j be an arbitrary pair of indices such that $1 \leq i < j \leq m$. Suppose $\mathfrak{p}_i = \mathfrak{p}_j$.

Choose l with $L_l \subset LL_iL_j$ and $l \neq i, j$. We have either $\mathfrak{p}_i = \mathfrak{p}_l$ or $\mathfrak{p}_i \neq \mathfrak{p}_l$. In the former case, L/L_+ would be ramified at a unique finite prime. Hence, Lemma 17 and Claim 4 would imply that h_L^- should be odd. Thus, Lemma 24 would imply $h_L^- \mid h_{LL_i}^-$, which contradicts the choice of L in the theorem.

In the latter case, a contradiction is obtained as follows: Let $M = LL_i$. (Then $M_+ = (L_jL_l)_+$ should hold.) The extension M/L would be ramified at $\mathfrak{p}_i$ since M_+/L_+ and L_i/L_+ were ramified at $\mathfrak{p}_i$. Therefore, M/L must be disjoint from H/L, where H is the 2-class field of L. Hence, we would get $[HM : M] = [H : L]$.

On the other hand, M_+ is associated with $\chi_j\chi_l$. Hence, Claim 4 and genus theory imply that h_{M_+} is odd. (A more precise description of M_+ is as follows: M/M_+ is the only quadratic extension of M_+ that is unramified at the finite primes.)

Since the 2-class field of M contains HM, the conclusions of the previous two paragraphs would imply that $[H : L]$ should divide h_M^-. Here, the order of 2 in $[H : L]$ equals the order of 2 in h_L^- by Claim 4. Hence, the order of 2 in h_L^- must be less than or equal to that of h_M^-. Now, Lemma 18 (or Lemma 24) would imply $h_L^- \mid h_M^-$, which contradicts the choice of L in the theorem.

The contradiction proves $\mathfrak{p}_i \neq \mathfrak{p}_j$. Since i and j are arbitrary, we get the desired claim.

Claim 8. *There are exactly four CM-extensions L, L_1, L_2 and L_3 of L_+ in K.*

Suppose $m \geq 4$. The Choice implies that L is associated with $\chi_1\chi_2\chi_3$. Hence, $\chi_i\chi_j\chi_4$ is not associated with L for $1 \leq i < j \leq 3$. However, $\chi_i\chi_j\chi_4$ would be associated with a CM-extension of L_+. By Claim 6, the conductor $\mathfrak{f}(\chi_i\chi_j\chi_4)$ would be a power of a finite prime. This contradicts Claim 7.

Claim 9. *The number of finite primes ramified in L/L_+ is* 3.

By the Choice, L/L_+ is associated with $\chi_1\chi_2\chi_3$. Hence, Claims 6 and 7 imply the desired claim.

Claim 10. *The* 2*-rank of $\mathcal{C}_L$ is* 2.

This follows from Claim 9 and Lemma 17.

Claim 11. $\mathrm{Im}(N : \mathcal{C}_{LL_1L_2L_3} \to \mathcal{C}_L) = \mathcal{C}_L^2$.

This follows from Claims 7 and 10. (Recall that L/L_+ is associated with $\chi_1\chi_2\chi_3$ and use the well known genus theory.)

Claims 4, 9, 10, 6, 5, 7, Choice, Claims 11 and 8 constitute the desired theorem. ∎

7. Proofs of main results. Now, we have enough tools for proving main results.

Proof of Theorem 1. Let $k \subset K$ be two CM-fields. As in Theorem 30, let L be a maximal intermediate field L of K/k such that $h_k^- \mid h_L^-$. It suffices to show $h_L^- \mid 4h_K^-$. If K does not contain a bicyclic biquadratic extension of L, then $h_k^- \mid 4h_K^-$ follows from Corollary 28. Assume that K contains a bicyclic biquadratic extension of L. By assertion (iii) of Theorem 30, the 2-rank of $\mathcal{C}_L$ is 2. By Lemma 24, we get $h_L^- \mid 4h_K^-$. ∎

Proof of Corollary 2. This is an easy consequence of Theorem 1. Note that $h_k = h_k^-$ since k is an imaginary quadratic field. ∎

Proof of Theorem 3. By Lemma 3 of [25], a zero in the specified region is necessarily simple. By Theorem 1 of [9], a positive simple zero of ζ_N comes from a simple zero of ζ_F for some quadratic subfield F of N. Corollary 2 and determination of class number 1, 2 and 4 in imaginary quadratic fields [1, 2, 3, 23, 24] gives a list of finitely many imaginary quadratic fields which can be contained in N. The largest conductor of these imaginary quadratic fields is 1555. However, it is shown in [18] that Dedekind zeta-functions of imaginary quadratic fields of conductors ≤ 593000 have no positive zero. Hence, F must be real. ∎

Remark. Arno's determination [1] of imaginary quadratic fields of class number 4 via [5, 6] is used in the above proof. However, transcendental number theory (estimates on logarithmic forms) is also applicable in our context. Arno [1] determines all imaginary quadratic fields of class number 4, among which there are several fields whose class groups are cyclic. On the other hand, the result of Whitaker [28] uses estimates on logarithmic forms for effective determination of imaginary quadratic fields that have prescribed prime divisors of discriminants and class groups isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. We verify that the result of [28] is suitable for our purpose if a numerical constant is made explicit: Let k be an imaginary quadratic subfield of a CM-field K of odd relative class number. Then Corollary 2 implies that h_k divides 4. By Lemma 25, the complex conjugation of k fixes $\mathcal{C}_k$. Hence, $\mathcal{C}_k$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ with $r = 0, 1$ or 2. If $r = 0$ or 1, then k belongs to the finite list of imaginary quadratic fields of class number 1 or 2, determined by Baker–Stark [2, 3, 23, 24] via estimates on logarithmic forms. Assume $r = 2$. Then the second remark to Lemma 26 (or an obvious refinement of Corollary 28) implies that K contains an unramified quadratic extension of k. Or equivalently, there is a decomposition $d = d_1 d_2$ of the discriminant d of k into pairwise coprime fundamental discriminants such that K contains $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Without loss of generality, we assume d_1 to be negative. Then the 2-rank of $\mathcal{C}_{\mathbb{Q}(\sqrt{d_1})}$ is smaller than that of $\mathcal{C}_k$ and hence is 0 or 1. By repeating the argument after application of Lemma 25 to k, we see $h_{\mathbb{Q}(\sqrt{d_1})}$ is 1 or 2 so that d_1 belongs to the finite list of Baker–Stark. Therefore, the smallest prime divisor of d is at most 163. Hence, [28] gives an effective upper bound on d. Replace K with a normal CM-field N.

References

[1] S. Arno, *The imaginary quadratic fields of class number* 4, Acta Arith. 60 (1992), 321–334.

[2] A. Baker, *A remark on the class number of quadratic fields*, Bull. London Math. Soc. 1 (1966), 98–102.

[3] —, *Imaginary quadratic fields with class number* 2, Ann. of Math. 94 (1971), 139–152.

[4] H. Furuya, *On divisibility by* 2 *of the relative class numbers of imaginary number fields*, Tôhoku Math. J. 23 (1971), 207–218.

[5] D. M. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa (4) 3 (1976), 623–663.

[6] B. Gross et D. Zagier, *Points de Heegner et derivées de fonctions L*, C. R. Acad. Sci. Paris 297 (1983), 85–87.

[7] K. Győry, *Sur une classe des corps de nombres algébriques et ses applications*, Publ. Math. Debrecen 22 (1975), 151–175.

[8] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. 56 (1952), 227–253.

[9] H. Heilbronn, *On real zeros of Dedekind ζ-functions*, Canad. J. Math. 25 (1973), 870–873.

[10] M. Hirabayashi and K. Yoshino, *Remarks on unit indices of imaginary abelian number fields II*, Manuscripta Math. 64 (1989), 235–251.

[11] J. Hoffstein, *Some analytic bounds for zeta functions and class numbers*, Invent. Math. 55 (1979), 37–47.

[12] K. Horie, *On a ratio between relative class numbers*, Math. Z. 211 (1992), 505–521.

[13] —, *On CM-fields with the same maximal real subfield*, Acta Arith. 67 (1994), 219–227.

[14] D. H. Lehmer, E. Lehmer and D. Shanks, *Integer sequences having prescribed quadratic character*, Math. Comp. 24 (1970), 433–451.

[15] F. Lemmermeyer, *Kuroda's class number formula*, Acta Arith. 66 (1994), 245–260.

[16] —, *Ideal class groups of cyclotomic number fields I*, ibid. 72 (1995), 347–359.

[17] —, *On* 2*-class field towers of some imaginary quadratic number fields*, Abh. Math. Sem. Univ. Hamburg 67 (1997), 205–214.

[18] M. E. Low, *Real zeros of the Dedekind zeta function of an imaginary quadratic field*, Acta Arith. 14 (1968), 117–140.

[19] H. L. Montgomery and P. J. Weinberger, *Notes on small class numbers*, ibid. 24 (1974), 529–542.

[20] P. Roquette, *On class field towers*, in: Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich (eds.), Academic Press, London, 1967, 231–249.

[21] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton Univ. Press, Princeton, 1997.

[22] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties*, The Mathematical Society of Japan, 1961.

[23] H. M. Stark, *A complete determination of the complex quadratic fields of class number one*, Michigan Math. J. 14 (1967), 1–27.

[24] —, *On complex quadratic fields with class number two*, Math. Comp. 29 (1975), 289–302.

[25] —, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.

[26] T. Takagi, *Über eine Theorie des relativ Abel'schen Zahlkörpers*, in: T. Takagi, Collected Papers, Springer, Tokyo, 1990, 73–167.

[27] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982, 2nd ed., 1991.

[28] E. E. Whitaker, *A determination of the imaginary quadratic number fields with Klein-four group as class group*, thesis, 1972.

Doshisha University
Department of Mathematics
Faculty of Engineering
Kyotanabe, Kyoto, 610-0321 Japan
E-mail: rokazaki@dd.iij4u.or.jp

Received on 3.6.1998
and in revised form on 17.5.1999 (3395)