IDEAL CLASS GROUPS OF CYCLOTOMIC NUMBER FIELDS I

FRANZ LEMMERMEYER

ABSTRACT. Following Hasse's example, various authors have been deriving divisibility properties of minus class numbers of cyclotomic fields by carefully examining the analytic class number formula. In this paper we will show how to generalize these results to CM-fields by using class field theory. Although we will only need some special cases, we have also decided to include a few results on Hasse's unit index for CM-fields as well, because it seems that our proofs are more direct than those in Hasse's book [2].

1. Notation

Let $K \subset L$ be number fields; we will use the following notation:

- $\mathcal{O}_K$ is the ring of integers of K;
- E_K is its group of units;
- W_K is the group of roots of unity contained in K;
- w_K is the order of W_K;
- $\mathrm{Cl}(K)$ is the ideal class group of K;
- $[\mathfrak{a}]$ is the ideal class generated by the ideal $\mathfrak{a}$;
- K^1 denotes the Hilbert class field of K, that is the maximal abelian extension of K that is unramified at all places;
- $j_{K\to L}$ denotes the transfer of ideal classes for number fields $K \subset L$, i.e. the homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(L)$ induced by mapping an ideal $\mathfrak{a}$ to $\mathfrak{a}\mathfrak{O}_L$;
- $\kappa_{L/K}$ denotes the capitulation kernel $\ker j_{K\to L}$;

Now let K be a CM-field, i.e. a totally complex quadratic extension of a totally real number field; the following definitions are standard:

- σ is complex conjugation;
- K^+ denotes the maximal real subfield of K; this is the subfield fixed by σ.
- $\mathrm{Cl}^-(K)$ is the kernel of the map $N_{K/K^+} : \mathrm{Cl}(K) \to \mathrm{Cl}(K^+)$ and is called the minus class group;
- $h^-(K)$ is the order of $\mathrm{Cl}^-(K)$, the minus class number;
- $Q(K) = (E_K : W_K E_{K^+}) \in \{1, 2\}$ is Hasse's unit index.

We will need a well known result from class field theory. Assume that $K \subset L$ are CM-fields; then $\ker(N_{L/K} : \mathrm{Cl}(L) \to \mathrm{Cl}(K))$ has order $(L \cap K^1 : K)$. Since K/K^+ is ramified at the infinite places, the norm $N_{K/K^+} : \mathrm{Cl}(K) \to \mathrm{Cl}(K^+)$ is onto.

2. Hasse's unit index

Hasse's book [2] contains numerous theorems (Sätze 14 – 29) concerning the unit index $Q(L) = (E_L : W_L E_K)$, where $K = L^+$ is the maximal real subfield of a

1991 *Mathematics Subject Classification.* Primary 11 R 18; Secondary 11 R 29.

Key words and phrases. Ideal class group, cyclotomic fields, unit index, class number formula.

cyclotomic number field L. Hasse considered only abelian number fields $L/\mathbb{Q}$, hence he was able to describe these fields in terms of their character groups $X(L)$; as we are interested in results on general CM-fields, we have to proceed in a different manner. But first we will collect some of the most elementary properties of $Q(L)$ (see also [2] and [13]; a reference "Satz ∗" always refers to Hasse's book [2]) in

Proposition 1. *Let $K \subset L$ be CM-fields; then*

a) *(Satz 14)* $Q(L) = (E_L : W_L E_{L^+}) = (E_L^{\sigma-1} : W_L^2) = (E_L^{\sigma+1} : E_{L^+}^2)$*; in particular,* $Q(L) \in \{1, 2\}$.
b) *(Satz 16, 17) if* $Q(L) = 2$ *then* $\kappa_{L/L^+} = 1$*;*
c) *(Satz 25) If* L^+ *contains units with any given signature, then* $Q(L) = 1$.
d) *(Satz 29)* $Q(K) | Q(L) \cdot (W_L : W_K)$*;*
e) *(compare Satz 26) Suppose that* $N_{L/K} : W_L/W_L^2 \to W_K/W_K^2$ *is onto. Then* $Q(L) \mid Q(K)$.
f) *(*[4, Lemma 2]*) If* $(L : K)$ *is odd, then* $Q(L) = Q(K)$*;*
g) *(Satz 27) If* $L = \mathbb{Q}(\zeta_m)$*, where* $m \not\equiv 2 \bmod 4$ *is composite, then* $Q(L) = 2$*;*
h) *(see Example 4 below) Let* $K_1 \subseteq \mathbb{Q}(\zeta_m)$ *and* $K_2 \subseteq \mathbb{Q}(\zeta_n)$ *be abelian CM-fields, where* $m = p^\mu$ *and* $n = q^\nu$ *are prime powers such that* $p \neq q$*, and let* $K = K_1K_2$*; then* $Q(K) = 2$.

The proofs are straight forward:

a) The map $\varepsilon \longrightarrow \varepsilon^{\sigma-1}$ induces an epimorphism $E_L \longrightarrow E_L^{\sigma-1}/W_L^2$. If $\varepsilon^{\sigma-1} = \zeta^2$ for some $\zeta \in W_L$, then $(\zeta\varepsilon)^{\sigma-1} = 1$, and $\zeta\varepsilon \in E_{L^+}$. This shows that $\sigma - 1$ gives rise to an isomorphism $E_L/W_LE_{L^+} \longrightarrow E_L^{\sigma-1}/W_L^2$, hence we have $(E_L : W_LE_{L^+}) = (E_L^{\sigma-1} : W_L^2)$. The other claim is proved similarly.
b) Since W_L/W_L^2 is cyclic of order 2, the first claim follows immediately from a). Now let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$ such that $\mathfrak{a}\mathcal{O}_L = \alpha\mathcal{O}_L$. Then $\alpha^{\sigma-1} = \zeta$ for some root of unity $\zeta \in L$, and $Q(L) = 2$ shows that $\zeta = \varepsilon^{\sigma-1}$ for some $\varepsilon \in E_L$. Now $\alpha\varepsilon^{-1}$ generates $\mathfrak{a}$ and is fixed by σ, hence lies in K. This shows that $\mathfrak{a}$ is principal in K, i.e. that $\kappa_{L/L^+} = 1$.
c) Units in L^+ that are norms from L are totally positive; our assumption implies that totally positive units are squares, hence we get $E_L^{\sigma+1} = E_{L^+}^2$, and our claim follows from a).
d) First note that $(W_L : W_K) = (W_L^2 : W_K^2)$; then
$$\begin{aligned} Q(L) \cdot (W_L : W_K) &= (E_L^{\sigma-1} : W_L^2)(W_L^2 : W_K^2) \\ &= (E_L^{\sigma-1} : E_K^{\sigma-1})(E_K^{\sigma-1} : W_K^2) \\ &= (E_L^{\sigma-1} : E_K^{\sigma-1}) \cdot Q(K) \end{aligned}$$
proves the claim.
e) Since $Q(L) = 2$, there is a unit $\varepsilon \in E_L$ such that $\varepsilon^{\sigma-1} = \zeta$ generates W_L/W_L^2. Taking the norm to K shows that $(N_{L/K}\varepsilon)^{\sigma-1} = N_{L/K}(\zeta)$ generates W_K/W_K^2, i.e. we have $Q(K) = 2$.
f) If $(L : K)$ is odd, then $(W_L : W_K)$ is odd, too, and we get $Q(K) \mid Q(L)$ from d) and $Q(L) \mid Q(K)$ from e).
g) In this case, $1 - \zeta_m$ is a unit, and we find $(1 - \zeta_m)^{1-\sigma} = -\zeta_m$. Since $-\zeta_m \in W_L \setminus W_L^2$, we must have $Q(L) = 2$;
h) First assume that m and n are odd. A subfield $F \subseteq L = \mathbb{Q}(\zeta_m)$, where $m = p^\mu$ is an odd prime power, is a CM-field if and only if it contains the maximal 2-extension contained in L, i.e. if and only $(L : F)$ is odd.

Since $(\mathbb{Q}(\zeta_m) : K_1)$ and $(\mathbb{Q}(\zeta_n) : K_2)$ are both odd, so is $(\mathbb{Q}(\zeta_{mn}) : K_1K_2)$; moreover, $\mathbb{Q}(\zeta_{mn})$ has unit index $Q = 2$, hence the assertion follows from f) and g).

Now assume that $p = 2$. If $\sqrt{-1} \in K_1$, then we must have $K_1 = \mathbb{Q}(\zeta_m)$ for $m = 2^\alpha$ and some $\alpha \geq 2$ (complex subfields of the field of 2^μth roots of unity containing $\sqrt{-1}$ necessarily have this form). Now n is odd and $K_2 \subseteq \mathbb{Q}(\zeta_n)$ is complex, hence $(\mathbb{Q}(\zeta_n) : K_2)$ is odd. By f) it suffices to show that $K_1(\zeta_n) = \mathbb{Q}(\zeta_{mn})$ has unit index 2, and this follows from g).

If $\sqrt{-1} \notin K_1$, let $\widetilde{K}_1 = K_1(i)$; then $\widetilde{K}_1 = \mathbb{Q}(\zeta_m)$ for $m = 2^\alpha$ and some $\alpha \geq 2$, and in the last paragraph we have seen that $Q(\widetilde{K}_1K_2) = 2$. Hence we only need to show that the norm map

$$N : W_{\widetilde{K}_1}/W_{\widetilde{K}_1}^2 \to W_{K_1}/W_{K_1}^2$$

is onto: since $(W_{\widetilde{K}_1K_2} : W_{\widetilde{K}_1})$ is odd, this implies $2 = Q(\widetilde{K}_1K_2) \mid Q(K_1K_2)$ by e). But the observation that the non-trivial automorphism of $\mathbb{Q}(\zeta_m)/K_1$ maps ζ_m to $-\zeta_m^{-1}$ implies at once that $N(\zeta_m) = -1$, and -1 generates $W_{K_1}/W_{K_1}^2$.

Now let L be a CM-field with maximal real subfield K; we will call L/K *essentially ramified* if $L = K(\sqrt{\alpha}\,)$ and there is a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ such that the exact power of $\mathfrak{p}$ dividing α is odd; it is easily seen that this does not depend on which α we choose. Moreover, every ramified prime ideal $\mathfrak{p}$ above an odd prime p is necessarily essentially ramified. We leave it as an exercise to the reader to verify that our definition of essential ramification coincides with Hasse's [2, Sect. 22]; the key observation is the ideal equation $(4\alpha) = \mathfrak{a}^2\mathfrak{d}$, where $\mathfrak{d} = \operatorname{disc}\,(K(\sqrt{\alpha}\,)/K)$ and $\mathfrak{a}$ is an integral ideal in $\mathcal{O}_K$.

We will also need certain totally real elements of norm 2 in the field of 2^mth roots of unity: to this end we define

$$\begin{aligned} \pi_2 &= 2 = 2 + \zeta_4 + \zeta_4^{-1}, \\ \pi_3 &= 2 + \sqrt{2} = 2 + \zeta_8 + \zeta_8^{-1}, \\ &\ldots, \\ \pi_n &= 2 + \sqrt{\pi_{n-1}} = 2 + \zeta_{2^n} + \zeta_{2^n}^{-1}. \end{aligned}$$

Let $m \geq 2$, $L = \mathbb{Q}(\zeta_{2^{m+1}})$ and $K = \mathbb{Q}(\pi_m)$; then L/K is an extension of type $(2,2)$ with subfields $K_1 = \mathbb{Q}(\zeta_{2^m})$, $K_2 = \mathbb{Q}(\sqrt{\pi_m})$ and $K_3 = \mathbb{Q}(\sqrt{-\pi_m})$. Moreover, K_2/K and K_3/K are essentially ramified, whereas K_1/K is not.

Theorem 1. *Let L be a CM-field with maximal real subfield K;*

- (i) *If $w_L \equiv 2 \bmod 4$, then*
  1. *If L/K is essentially ramified, then $Q(L) = 1$, and $\kappa_{L/K} = 1$.*
  2. *L/K is not essentially ramified. Then $L = K(\sqrt{\alpha}\,)$ for some $\alpha \in \mathcal{O}_K$ such that $\alpha\mathcal{O}_K = \mathfrak{a}^2$, where $\mathfrak{a}$ is an integral ideal in $\mathcal{O}_K$. Now*
     - (a) *$Q(L) = 2$, if $\mathfrak{a}$ is principal, and*
     - (b) *$Q(L) = 1$ and $\kappa_{L/K} = \langle[\mathfrak{a}]\rangle$, if $\mathfrak{a}$ is not principal.*
- (ii) *If $w_L \equiv 2^m \bmod 2^{m+1}$, where $m \geq 2$ then L/K is not essentially ramified, and*
  1. *if $\pi_m\mathcal{O}_K$ is not an ideal square, then $Q(L) = 1$ and $\kappa_{L/K} = 1$;*

2. *if* $\pi_m\mathcal{O}_K = \mathfrak{b}^2$ *for some integral ideal* $\mathfrak{b}$*, then*
   (a) $Q(L) = 2$*, if* $\mathfrak{b}$ *is principal, and*
   (b) $Q(L) = 1$*,* $\kappa_{L/K} = \langle[\mathfrak{b}]\rangle$*, if* $\mathfrak{b}$ *is not principal.*

For the proof of Theorem 1 we will need the following

Lemma 1. *Let* $L = K(\sqrt{\pi}\,)$*, and let* σ *denote the non-trivial automorphism of* L/K*. Moreover, let* $\mathfrak{b}$ *be an ideal in* $\mathcal{O}_K$ *such that* $\mathfrak{b}\mathcal{O}_L = (\beta)$ *and* $\beta^{\sigma-1} = -1$ *for some* $\beta \in L$*. Then* $\pi\mathcal{O}_K$ *is an ideal square in* $\mathcal{O}_K$*.*

If, on the other hand, $\beta^{\sigma-1} = \zeta$*, where* ζ *is a primitive* 2^m*th root of unity, then* $\pi_m\mathcal{O}_K$ *is an ideal square in* $\mathcal{O}_K$*.*

Proof. We have $(\beta\sqrt{\pi}\,)^{\sigma-1} = 1$, hence $\beta\sqrt{\pi} \in K$. Therefore $\mathfrak{b}$ and $\mathfrak{c} = (\beta\sqrt{\pi}\,)$ are ideals in $\mathcal{O}_K$, and $(\mathfrak{c}\mathfrak{b}^{-1})^2 = \pi\mathcal{O}_K$ proves our claim.

Now assume that $\beta^{\sigma-1} = \zeta$; then σ fixes $(1-\zeta)\beta^{-1}$, hence $((1-\zeta)\beta)$ and $\mathfrak{c} = (1-\zeta) = \mathfrak{c}^\sigma$ are ideals in $\mathcal{O}_K$, and $\mathfrak{c}^2 = N_{L/K}(1-\zeta) = (2+\zeta+\zeta^{-1})\mathcal{O}_K$ is indeed an ideal square in $\mathcal{O}_K$ as claimed. $\square$

Proof of Theorem 1. There are the following cases to consider:

(i) Assume that $w_L \equiv 2 \bmod 4$.

1. L/K is essentially ramified.
   Assume we had $Q(L) = 2$; then $E_L^{\sigma-1} = W_L$, hence there is a unit $\varepsilon \in E_L$ such that $\varepsilon^{\sigma-1} = -1$. Write $L = K(\sqrt{\pi}\,)$, and apply Lemma 1 to $\mathfrak{b} = (1), \beta = \varepsilon$: this will yield the contradiction that L/K is not essentially ramified.
2. L/K is not essentially ramified.
   Then $L = K(\sqrt{\alpha}\,)$ for some $\alpha \in \mathcal{O}_K$ such that $\alpha\mathcal{O}_K = \mathfrak{a}^2$, where $\mathfrak{a}$ is an integral ideal in $\mathcal{O}_K$.
   (a) If $\mathfrak{a}$ is principal, say $\mathfrak{a} = \beta\mathcal{O}_K$, then there is a unit $\varepsilon \in E_K$ such that $\alpha = \beta^2\varepsilon$, and we see that $L = K(\sqrt{\varepsilon}\,)$. Now $\sqrt{\varepsilon}^{\,\sigma-1} = -1$ is no square since $w_L \equiv 2 \bmod 4$, and Prop. 1.a) gives $Q(L) = 2$.
   (b) If $\mathfrak{a}$ is not principal, then the ideal class $[\mathfrak{a}]$ capitulates in L/K because $\mathfrak{a}\mathcal{O}_L = \sqrt{\alpha}\mathcal{O}_L$. Prop. 1.b) shows that $Q(L) = 1$.

(ii) Assume that $w_L \equiv 2^m \bmod 2^{m+1}$ for some $m \ge 2$.

1. If we have $Q(L) = 2$ or $\kappa_{L/K} \ne 1$, then Lemma 1 says that $\pi_m\mathcal{O}_K = \mathfrak{b}^2$ is an ideal square in $\mathcal{O}_K$ in contradiction to our assumption.
2. Suppose therefore that $\pi_m = \mathfrak{b}^2$ is an ideal square in $\mathcal{O}_K$. If $\mathfrak{b}$ is not principal, then $\mathfrak{b}\mathcal{O}_L = (1-\zeta)$ shows that $\kappa_{L/K} = \langle[\mathfrak{b}]\rangle$, and Prop. 1.b) gives $Q(L) = 1$. If, on the other hand, $\mathfrak{b} = \beta\mathcal{O}_K$, then $\eta\beta^2 = \pi_m$ for some unit $\eta \in E_K$. If η were a square in $\mathcal{O}_K$, then π_m would also be a square, and $L = K(\sqrt{-1}\,)$ would contain the 2^{m+1}th roots of unity. Now $\eta\beta^2 = \pi_m = \zeta^{-1}(1+\zeta)^2$, hence $\eta\zeta$ is a square in L, and we have $Q(L) = 2$ as claimed.

$\square$

Remark. For $L/\mathbb{Q}$ abelian, Theorem 1 is equivalent to Hasse's Satz 22; we will again only sketch the proof: suppose that $w_L \equiv 2^m \bmod 2^{m+1}$ for some $m \ge 2$, and define $L' = L(\zeta_{2^{m+1}})$, $K' = L' \cap \mathbb{R}$. Then K'/K is essentially ramified if and only if π_m is not an ideal square in $\mathcal{O}_K$ (because $K' = K(\pi_{m+1}) = K(\sqrt{\pi_m})$). The asserted equivalence should now be clear. Except for the results on capitulation, Theor. 1 is also contained in [10] (for general CM-fields).

Examples.

1. Complex subfields L of $\mathbb{Q}(\zeta_{p^m})$, where p is prime, have unit index $Q(L) = 1$ (Hasse's Satz 23) and $\kappa_{L/L^+} = 1$: since p ramifies completely in $\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}$, L/L^+ is essentially ramified if $p \neq 2$, and the claim follows from Theorem 1. If $p = 2$ and L/L^+ is not essentially ramified, then we must have $L = \mathbb{Q}(\zeta_{2^\mu})$ for some $\mu \in \mathbb{N}$, and we find $Q(L) = 1$ by Theorem 1.2.1.

2. $L = \mathbb{Q}(\zeta_m)$ has unit index $Q(L) = 1$ if and only if $m \not\equiv 2 \bmod 4$ is a prime power (Satz 27). This follows from Example 1. and Prop. 1.e)

3. If K is a CM-field, which is essentially ramified at a prime ideal $\mathfrak{p}$ above $p \in \mathbb{N}$, and if F is a totally real field such that $p \nmid \operatorname{disc} F$, then $Q(L) = 1$ and $\kappa_{L/L^+} = 1$ for $L = KF$: this is again due to the fact that either L/L^+ is essentially ramified at the prime ideals above $\mathfrak{p}$, or $p = 2$ and $K = K^+(\sqrt{-1}\,)$. In the first case, we have $Q(L) = 1$ by Theorem 1.1.1, and in the second case by Theorem 1.2.1.

4. Suppose that the abelian CM-field K is the compositum $K = K_1 \ldots K_t$ of fields with pairwise different prime power conductors; then $Q(K) = 1$ if and only if exactly one of the K_i is imaginary. (Uchida [12, Prop. 3]) The proof is easy: if there is exactly one complex field among the K_j, then $Q(K) = 1$ by Example 3. Now suppose that K_1 and K_2 are imaginary; we know $Q(K_1K_2) = 2$ (Prop. 1.h), and from the fact that the K_j have pairwise different conductors we deduce that $(W_K : W_{K_1K_2}) \equiv 1 \bmod 2$. Now the claim follows from Hasse's Satz 29 (Prop. 1.c). Observe that $\kappa_{K/K^+} = 1$ in all cases.

5. Cyclic extensions $L/\mathbb{Q}$ have unit index $Q(L) = 1$ (Hasse's Satz 24): Let F be the maximal subfield of L such that $(F : \mathbb{Q})$ is odd. Then F is totally real, and $2 \nmid \operatorname{disc} F$ (this follows from the theorem of Kronecker and Weber). Similarly, let K be the maximal subfield of L such that $(K : \mathbb{Q})$ is a 2-power: then K is a CM-field, and $L = FK$. If K/K^+ is essentially ramified at a prime ideal $\mathfrak{p}$ above an odd prime p, then so is L/L^+, because $L/\mathbb{Q}$ is abelian, and all prime ideals in F have odd ramification index. Hence the claim in this case follows by Example 3. above.

If, however, K/K^+ is not essentially ramified at a prime ideal $\mathfrak{p}$ above an odd prime p, then $\operatorname{disc} K$ is a 2-power (recall that $K/\mathbb{Q}$ is cyclic of 2-power degree). Applying the theorem of Kronecker and Weber, we find that $K \subseteq \mathbb{Q}(\zeta)$, where ζ is some primitive 2^mth root of unity. If K/K^+ is essentially ramified at a prime ideal above 2, then so is L/L^+, and Theorem 1 gives us $Q(L) = 1$. If K/K^+ is not essentially ramified at a prime ideal above 2, then we must have $K = \mathbb{Q}(\zeta)$, where ζ is a primitive 2^mth root of unity; but now $\pi_m\mathcal{O}_{L^+}$ is not the square of an integral ideal, and we have $Q(L) = 1$ by Theorem 1. Alternatively, we may apply Prop. 1.e) and observe that $Q(K) = 1$ by Example 1.

6. Let $p \equiv 1 \bmod 8$ be a prime such that the fundamental unit ε_{2p} of $\mathbb{Q}(\sqrt{2p}\,)$ has norm $+1$ (by [11], there are infinitely many such primes; note also that $N\varepsilon_{2p} = +1 \iff (2, \sqrt{2p}\,)$ is principal). Put $K = \mathbb{Q}(i, \sqrt{2p}\,)$ and $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{p}\,)$. Then $Q(K) = 2$ by Theor. 1.2.2.a), whereas the fact that L is the compositum of $\mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(\sqrt{p}\,)$ shows that $Q(L) = 1$ (Example 4). This generalization of Lenstra's example given by Martinet in [2] is contained in Theor. 4 of [4], where several other results of this kind can be found.

3. Masley's theorem $h_m^-|h_{mn}^-$

Now we can prove a theorem that will contain Masley's result $h^-(K)\,|\,h^-(L)$ for cyclotomic fields $K=\mathbb{Q}(\zeta_m)$ and $L=\mathbb{Q}(\zeta_{mn})$ as a special case:

Theorem 2. *Let $K\subset L$ be CM-fields; then*

$$h^-(K)\,|\,h^-(L)\cdot|\kappa_{L/L^+}|\cdot\frac{(L\cap K^1:K)}{(L^+\cap(K^+)^1:K^+)},$$

and the last quotient is a power of 2.

Proof. Let ν_K and ν_L denote the norms N_{K/K^+} and N_{L/L^+}, respectively; then the following diagram is exact and commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Cl}^-(L) & \longrightarrow & \mathrm{Cl}(L) & \xrightarrow{\nu_L} & \mathrm{Cl}(L^+) & \longrightarrow & 1 \\ & & \big\downarrow{\scriptstyle N^-} & & \big\downarrow{\scriptstyle N} & & \big\downarrow{\scriptstyle N^+} & & \\ 1 & \longrightarrow & \mathrm{Cl}^-(K) & \longrightarrow & \mathrm{Cl}(K) & \xrightarrow{\nu_K} & \mathrm{Cl}(K^+) & \longrightarrow & 1 \end{array}$$

The snake lemma gives us an exact sequence

$$\begin{array}{l} 1 \longrightarrow \ker N^- \longrightarrow \ker N \longrightarrow \ker N^+ \\ \qquad \longrightarrow \operatorname{cok} N^- \longrightarrow \operatorname{cok} N \longrightarrow \operatorname{cok} N^+ \longrightarrow 1. \end{array}$$

Let $h(L/K)$ denote the order of $\ker N$, and let $h^-(L/K)$ and $h(L^+/K^+)$ be defined accordingly. The remark at the end of Sect. 1 shows

$$|\operatorname{cok} N\,| = (L\cap K^1:K), \quad |\operatorname{cok} N^+\,| = (L^+\cap(K^+)^1:K^+).$$

The alternating product of the orders of the groups in exact sequences equals 1, so the above sequence implies

$$h^-(L/K)\cdot h(L^+/K^+)\cdot|\operatorname{cok} N| = h(L/K)\cdot|\operatorname{cok} N^-|\cdot|\operatorname{cok} N^+|.$$

The exact sequence

$$1\to\ker N^-\to\mathrm{Cl}^-(L)\to\mathrm{Cl}^-(K)\to\operatorname{cok} N^-\to 1$$

gives us

$$h^-(L/K)\cdot h^-(K) = h^-(L)\cdot|\operatorname{cok} N^-|.$$

Collecting everything we find that

$$h^-(K)\cdot\frac{h(L/K)}{h(L^+/K^+)}\cdot\frac{(L^+\cap(K^+)^1:K^+)}{(L\cap K^1:K)} = h^-(L) \tag{1}$$

Now the claimed divisibility property follows if we can prove that $h(L^+/K^+)$ divides $h(L/K)\cdot|\,\kappa_{L/L^+}|$. But this is easy: exactly $h(L^+/K^+)/|\,\kappa_{L/L^+}\,|$ ideal classes of $\ker N^+\subset\mathrm{Cl}(L^+)$ survive the transfer to $\mathrm{Cl}(L)$, and if the norm of L^+/K^+ kills an ideal class $c\in\mathrm{Cl}(L^+)$, the same thing happens to the transferred class c^j when the norm of L/K is applied. We remark in passing that $|\,\kappa_{L/L^+}\,|\le 2$ (see Hasse [2, Satz 18]).

It remains to show that $(L\cap K^1:K)/(L^+\cap(K^+)^1:K^+)$ is a power of 2. Using induction on $(L:K)$, we see that it suffices to prove: if L/K is an unramified abelian extension of CM-fields of odd prime degree $(L:K)=q$, then so is L^+/K^+. Suppose otherwise; then there exists a finite prime $\mathfrak{p}$ which ramifies, and since L^+/K^+ is cyclic, $\mathfrak{p}$ has ramification index q. Now L/K^+ is cyclic of order $2q$, hence K must be the inertia field of $\mathfrak{p}$, contradicting the assumption that L/K be unramified. We conclude that L^+/K^+ is also unramified, and so odd factors of $(L \cap K^1 : K)$ cancel against the corresponding factors of $(L^+ \cap (K^+)^1 : K^+)$. $\square$

Corollary 1 (Louboutin and Okazaki [7])**.** *Let $K \subset L$ be CM-fields such that $(L:K)$ is odd; then $h^-K \mid h^-(L)$.*

Proof. From (1) and the fact that $(L^+ \cap (K^+)^1 : K^+) = 1$ (this index is a power of 2 and divides $(L:K)$, which is odd), we see that it is sufficent to show that $h(L^+/K^+) \mid h(L/K)$. This in turn follows if we can prove that no ideal class from $\ker N^+ \subseteq \mathrm{Cl}(L^+)$ capitulates when transferred to $\mathrm{Cl}(L)$. Assume therefore that $\kappa_{L/L^+} = \langle [\mathfrak{a}] \rangle$. If $w_L \equiv 2 \bmod 4$, then by Theor. 1.1.2 we may assume that $L = L^+(\sqrt{\alpha}\,)$, where $\alpha \mathcal{O}_{L^+} = \mathfrak{a}^2$. Since $(L:K)$ is odd, we can choose $\alpha \in O_{K^+}$, hence $N^+(\mathfrak{a}) = \mathfrak{a}^{(L:K)}$ shows that the ideal class $[\mathfrak{a}]$ is not contained in $\ker N^+$. The proof in the case $w_L \equiv 0 \bmod 4$ is completely analogous. $\square$

Remark. For any prime p, let $\mathrm{Cl}_p^-(K)$ denote the p-Sylow subgroup of $\mathrm{Cl}^-(K)$; then $\mathrm{Cl}_p^-(K) \subseteq \mathrm{Cl}_p^-(L)$ for every $p \nmid (L:K)$. This is trivial, because ideal classes with order prime to $(L:K)$ cannot capitulate in L/K.

Corollary 2 (Masley [9])**.** *If $K = \mathbb{Q}(\zeta_m)$ and $L = \mathbb{Q}(\zeta_{mn})$ for some $m,n \in \mathbb{N}$, then $h^-(K) \mid h^-(L)$.*

Proof. We have shown in Sect. 2 that $j_{K^+ \to K}$ and $j_{L^+ \to L}$ are injective in this case. Moreover, L/K does not contain a nontrivial subfield of K^1 (note that p is completely ramified in L/K if $n = p$, and use induction). $\square$

The special case $m = p^a$, $n = p$ of Corollary 2 can already be found in [14]. Examples of CM-fields L/K such that $h^-(K) \nmid h^-(L)$ have been given by Hasse [2]; here are some more:

(1) Let $d_1 \in \{-4, -8, -q \ (q \equiv 3 \bmod 4)\}$ be a prime discriminant, and suppose that $d_2 > 0$ is the discriminant of a real quadratic number field such that $(d_1, d_2) = 1$. Put $K = \mathbb{Q}(\sqrt{d_1 d_2}\,)$ and $L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}\,)$; then $Q(L) = 1$ and $\kappa_{L/L^+} = 1$ by Example 4, and $(L \cap K^1 : K) = 2 \cdot (L^+ \cap (K^+)^1 : K^+)$ since L/K is unramified but L^+/K^+ is not. The class number formula (1) below shows that in fact $h^-(K) \nmid h^-(L)$.

(2) Let $d_1 = -4, d_2 = 8m$ for some odd $m \in \mathbb{N}$, and suppose that $\mathfrak{z} = (2, \sqrt{2m}\,)$ is not principal in $\mathcal{O}_k$, where $k = \mathbb{Q}(\sqrt{2m}\,)$. Then $h^-(K) \nmid h^-(L)$ for $K = \mathbb{Q}(\sqrt{-2m}\,)$, $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2m}\,)$. Here $(L \cap K^1 : K) = (L^+ \cap (K^+)^1 : K^+)$, but $\kappa_{L/L^+} = \langle [\mathfrak{z}] \rangle$, since $\mathfrak{z}\mathcal{O}_L = (1+i)$. This example shows that we cannot drop the factor κ_{L/L^+} in Theor. 2.

Other examples can be found by replacing d_1 in Example 2. by $d_1 = -8$ or d_2 by $d_2 = 4m, m \in \mathbb{N}$ odd. The proof that in fact $h^-(K) \nmid h^-(L)$ for these fields uses Theorem 1, as well as Prop. 2 and 3 below.

4. Metsänkylä's factorization

An extension L/K is called a V_4-extension of CM-fields if

(1) L/K is normal and $\mathrm{Gal}(L/K) \simeq V_4 = (2,2)$;
(2) Exactly two of the three quadratic subfields are CM-fields; call them K_1 and K_2, respectively.

This implies, in particular, that K is totally real, and that L is a CM-field with maximal real subfield $L^+ = K_3$. We will write $Q_1 = Q(K_1), W_1 = W_{K_1}$, etc.

Louboutin [6, Prop. 13] has given an analytic proof of the following class number formula for V_4-extension of CM-fields, which contains Lemma 8 of Ferrero [1] as a special case:

Proposition 2. *Let L/K be a V_4-extension of CM-fields; then*

$$h^-(L) = \frac{Q(L)}{Q_1Q_2}\frac{w_L}{w_1w_2}h^-(K_1)h^-(K_2).$$

Proof. Kuroda's class number formula (for an algebraic proof see [5]) yields

$$h(L) = 2^{d-\kappa-2-\upsilon}q(L)h(K_1)h(K_2)h(L^+)/h(K)^2, \tag{2}$$

where

- $d = (K : \mathbb{Q})$ is the number of infinite primes of K that ramify in L/K;
- $\kappa = d - 1$ is the $\mathbb{Z}$-rank of the unit group of K;
- $\upsilon = 1$ if and only if all three quadratic subfields of L/K can be written as $K(\sqrt{\varepsilon}\,)$ for units $\varepsilon \in E_K$, and $\upsilon = 0$ otherwise;
- $q(L) = (E_L : E_1E_2E_3)$ is the unit index for extensions of type $(2, 2)$; here E_j is the unit group of K_j (similarly, let W_j denote the group of roots unity in L_j).

Now we need to find a relation between the unit indices involved; we claim

Proposition 3. *If L/K is a V_4-extension of CM-fields, then*

$$\frac{Q(L)}{Q_1Q_2}\frac{w_L}{w_1w_2} = 2^{-1-\upsilon}q(L).$$

Plugging this formula into equation (2) and recalling $h^-(F) = h(F)/h(F^+)$ for CM-extensions F/F^+ yields Louboutin's formula. □

Proof of Prop. 3. We start with the observation

$$Q(L) = (E_L : W_LE_3) = (E_L : E_1E_2E_3)\frac{(E_1E_2E_3 : W_1W_2E_3)}{(W_LE_3 : W_1W_2E_3)}.$$

In [5] we have defined groups $E_j^* = \{\varepsilon \in E_j : N_j\varepsilon \text{ is a square in } E_K\}$, where N_j denotes the norm of K_j/K; we also have shown that

$$(E_1E_2E_3 : E_1^*E_2^*E_3^*) = 2^{-\upsilon}\prod(E_j : E_j^*)$$

and $E_j/E_j^* \simeq E_K/N_jE_j$. Now Prop. 1.a) gives $(E_K : N_jE_j) = Q_j$ for $j = 1, 2$, and we claim

1. $(W_LE_3 : W_1W_2E_3) = (W_L : W_1W_2) = 2 \cdot \frac{w_L}{w_1w_2}$;
2. $E_1^*E_2^*E_3^* = W_1W_2E_3^*$;
3. $(W_1W_2E_3 : W_1W_2E_3^*) = (E_3 : E_3^*)$.

This will give us

$$Q(L) = 2^{-1-\upsilon}q(L)Q_1Q_2\frac{w_1w_2}{w_L}, \tag{3}$$

completing the proof of Prop. 3 except for the three claims above:

1. $W_LE_3/W_1W_2E_3 \simeq W_L/(W_L \cap W_1W_2E_3) \simeq W_L/W_1W_2$, and the claim follows from $W_1 \cap W_2 = \{-1, +1\}$;

(2) We only need to show that $E_1^* E_2^* E_3^* \subset W_1 W_2 E_3^*$; but Prop. 1.a) shows that $\varepsilon \in E_1^* \iff \varepsilon^{\sigma+1} \in E_K^2 \iff \varepsilon \in W_1 E_K$, and this implies the claim;
(3) $W_1 W_2 E_3 / W_1 W_2 E_3^* \simeq E_3 / E_3 \cap W_1 W_2 E_3^* \simeq E_3 / E_3^*$.

□

Combining the result of Section 3 with Prop. 2, we get the following

Theorem 3. *Let L_1 and L_2 be CM-fields, and let $L = L_1 L_2$ and $K = L_1^+ L_2^+$; then L/K is a V_4-extension of CM-fields with subfields $K_1 = L_1 L_2^+$, $K_2 = L_1^+ L_2$, $K_3 = L^+$, and*

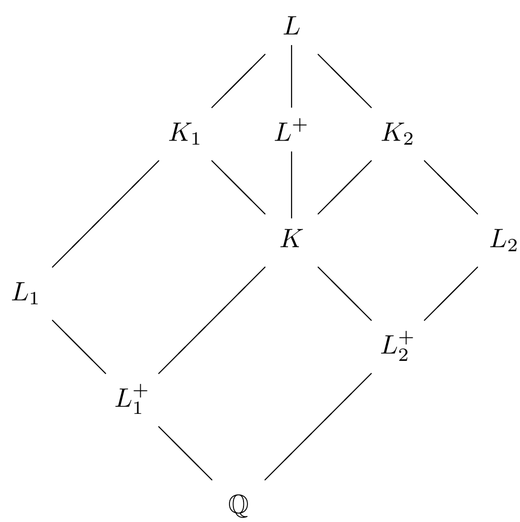
$$h^-(L) = \frac{Q(L)}{Q_1 Q_2} \frac{w_L}{w_1 w_2} h^-(L_1) h^-(L_2) T_1 T_2,$$

where $T_1 = h^-(L_1 L_2^+)/h^-(L_1)$ and $T_2 = h^-(L_2 L_1^+)/h^-(L_2)$.
If we assume that $\kappa_1 = \kappa_2 = 1$ (κ_1 is the group of ideal classes capitulating in $L_1 L_2^+/K$, κ_2 is defined similarly) and that

$$\begin{aligned} (L_1 L_2^+ \cap L_1^1 : L_1) &= (L_1^+ L_2^+ \cap (L_1^+)^1 : L_1^+), \\ (L_2 L_1^+ \cap L_2^1 : L_2) &= (L_2^+ L_1^+ \cap (L_2^+)^1 : L_2^+), \end{aligned}$$

then T_1 and T_2 are integers.

Proof. Theorem 3 follows directly from Theorem 2 and Proposition 2. □



Now let $m = p^\mu$ and $n = q^\nu$ be prime powers, and suppose that $p \neq q$ Moreover, let $L_1 \subseteq \mathbb{Q}(\zeta_m)$ and $L_2 \subseteq \mathbb{Q}(\zeta_n)$ be CM-fields. Then

(1) $Q(L) = 2$, $Q_1 = Q(L_1 L_2^+) = Q_2 = Q(L_2 L_1^+) = 1$: this has been proved in Prop. 1.h) and Example 4 in Sect. 2;
(2) $w_1 w_2 = 2 w_L$ (obviously);
(3) $\kappa_1 = \kappa_2 = 1$: see Example 4 in Sect. 2;
(4) $(L_1 L_2^+ \cap L_1^1 : L_1) = (L_1^+ L_2^+ \cap (L_1^+)^1 : L_1^+)$: this, as well as the corresponding property for K_2, is obvious, because the prime ideals above p and q ramify completely in L/L_2 and L/L_1, respectively.

In particular, we have the following

Corollary 3. *(Metsänkylä) Let $L_1 \subseteq \mathbb{Q}(\zeta_m)$ and $L_2 \subseteq \mathbb{Q}(\zeta_n)$ be CM-fields, where $m = p^\mu$ and $n = q^\nu$ are prime powers, and let $L = L_1L_2$; then*

$$h^-(L) = h^-(L_1)h^-(L_2)T_1T_2,$$

where $T_1 = h^-(L_1L_2^+)/h^-(L_1)$ and $T_2 = h^-(L_2L_1^+)/h^-(L_2)$ are integers.

It still remains to identify the character sums T_{01} and T_{10} in [8] with the class number factors T_1 and T_2 given above. But this is easy: the character group $X(L_1)$ corresponding to the field L_1 is generated by a character χ_1, and it is easily seen that

$$\begin{array}{rclrcl} X(L_1) & = & \langle\chi_1\rangle, & X(L_1L_2^+) & = & \langle\chi_1, \chi_2^2\rangle, \\ X(L_2) & = & \langle\chi_2\rangle, & X(L_2L_1^+) & = & \langle\chi_2, \chi_1^2\rangle, \\ X(L) & = & \langle\chi_1, \chi_2\rangle, & X(L^+) & = & \langle\chi_1\chi_2, \chi_1^2\rangle. \end{array}$$

The analytical class number formula for an abelian CM-field K reads

$$h^-(K) = Q(K)w_K \prod_{\chi\in X^-(K)} \frac{1}{2\mathfrak{f}(\chi)} \sum_{a \bmod^+ \mathfrak{f}(\chi)} (-\chi(a)a), \tag{4}$$

where $a \bmod^+ \mathfrak{f}(\chi)$ indicates that the sum is extended over all $1 \le a \le \mathfrak{f}(\chi)$ such that $(a, \mathfrak{f}(\chi)) = 1$, and $X^-(L) = X(L) \setminus X(L^+)$ is the set of $\chi \in X(L)$ such that $\chi(-1) = -1$. Applying formula (4) to the CM-fields listed above and noting that $Q(L) = 2$, $Q(L_1) = Q(L_2) = Q(L_1L_2^+) = Q(L_2L_1^+) = 1, 2w_L = w_1w_2$, we find

$$h^-(L) = h^-(L_1) \cdot h^-(L_2) \prod_{\chi\in X^*(L)} \frac{1}{2\mathfrak{f}(\chi)} \sum_{a \bmod^+ \mathfrak{f}(\chi)} (-\chi(a)a),$$

where $X^*(L)$ is the subset of all $\chi \in X^-(L)$ not lying in $X^-(L_1)$ or $X^-(L_2)$. Now define $X_1(L) = \{\chi = \chi_1^x\chi_2^y \in X^*(L) : x \equiv 1 \bmod 2,\ y \equiv 0 \bmod 2\}$, and let $X_2(L)$ be defined accordingly. Then $X^*(L) = X_1(L) \cup X_2(L)$, and

$$h^-(L_1) \cdot \prod_{\chi\in X_1(L)} \frac{1}{2\mathfrak{f}(\chi)} \sum_{a \bmod^+ \mathfrak{f}(\chi)} (-\chi(a)a) = h^-(L_1L_2^+),$$

and we have shown that

$$T_1 = \prod_{\chi\in X_1(L)} \frac{1}{2\mathfrak{f}(\chi)} \sum_{a \bmod^+ \mathfrak{f}(\chi)} (-\chi(a)a).$$

Comparing with the definition of Metsänkylä's factor T_{10}, this shows that indeed $T_1 = T_{10}$.

Acknowledgement

I would like to thank Stéphane Louboutin and Ryotaro Okazaki as well as Tauno Metsänkylä for several helpful suggestions and for calling my attention to the papers of Horie [3] and Uchida [12].

References

[1] B. Ferrero, *The cyclotomic $\mathbb{Z}_2-$extension of imaginary quadratic number fields*, American J. Math. **102** (1980), 447–459 8

[2] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Springer Verlag 1985 1, 2, 3, 5, 6, 7

[3] K. Horie *On a ratio between relative class numbers*, Math. Z. **211** (1992), 505–521 10

[4] M. Hirabayashi), K. Yoshino *Remarks on unit indices of imaginary abelian number fields*, Manuscripta Math. **60** (1988), 423–436 2, 5

[5] F. Lemmermeyer, *Kuroda's class number formula*, Acta Arith. **66** (1994), 245–260 8

[6] S. Louboutin, *Determination of all quaternion octic CM-fields with class number 2*, preprint 8

[7] S. Louboutin, M. Olivier, *The class number one problem for some non-abelian normal CM-fields*, preprint 1994 7

[8] T. Metsänkylä, *Über den ersten Faktor der Klassenzahl des Kreiskörpers*, Ann. Acad. Sci. Fenn. Ser. A. I **416** (1967) 10

[9] J. M. Masley, H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256 7

[10] R. Okazaki, *On evaluation of L-functions over real quadratic fields*, J. Math. Kyoto Univ. **31** (1991), 1125–1153 5

[11] A. Scholz, *Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$*, Math. Z. **39** (1934), 95–111 5

[12] K. Uchida, *Imaginary quadratic number fields with class number one*, Tohoku Math. Journ. **24** (1972), 487–499 5, 10

[13] L. Washington, *Introduction to Cyclotomic Fields*, Springer Verlag 1982 2

[14] J. Westlund, *On the class number of the cyclotomic number field*, Trans. Amer. Math. Soc. **4** (1903), 201–212 7

Bilkent University, Department of Mathematics, 06800 Bilkent, Ankara
E-mail address: `franz@fen.bilkent.edu.tr`