ACTA ARITHMETICA
131.3 (2008)

Ideal class groups of cyclotomic number fields III

by

Franz Lemmermeyer (Jagstzell)

9. Introduction. One of the most basic results in algebraic number theory is the fact that, in every finite extension $K/\mathbb{Q}$ of the rationals, at least one prime ramifies, i.e., that $|\operatorname{disc} K| > 1$ except when $K = \mathbb{Q}$. This lower bound for the discriminant was conjectured by Kronecker and first proved by Minkowski, whose geometric methods gave the more precise bound

$$|\operatorname{disc} K| \ge \left[\left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}\right]^2$$

for number fields of degree $(K : \mathbb{Q}) = n = r + 2s$ with exactly r real embeddings. Asymptotically, this shows that the root discriminant

$$\operatorname{rd}(K) = |\operatorname{disc} K|^{1/n}$$

of a number field satisfies $\operatorname{rd}(K) > e^2$ for large n. Blichfeldt [2, 3] was able to show that $\operatorname{rd}(K) > \pi e$ for large n, and that $\operatorname{rd}(K) > 2\pi e^{3/2}$ if K is totally real, and these bounds were later improved by Rogers [19, 20].

One possible approach to answering Furtwängler's question whether the class field tower always terminates was to show that $\operatorname{rd}(K)$ goes to infinity with n, because fields in the class field tower have constant root discriminant. In his article [22], Arnold Scholz asked how good the asymptotic bounds given above are. He denoted by k_n a number field of degree n whose absolute value of the discriminant is minimal, and put $E_n = |\operatorname{disc} k_n|^{1/n}$ (this is the root discriminant of k_n). He observed that the fields $\mathbb{Q}(\sqrt[n]{2})$ provided the upper bound $E_n < 2n$. He conjectured that $\lim E_n/n = 0$ and proved that in fact $E_n < (\log n)^2$ for certain n by constructing number fields of small discriminant. This was accomplished by studying the ray class field $k\{(p)\}$ modulo (p) of $k = \mathbb{Q}(\zeta_{p-1})$.

2000 *Mathematics Subject Classification*: Primary 11R21; Secondary 11R29, 11R18.
Key words and phrases: unramified extension, ideal group, ray class field, cyclotomic field.

In this article we will show that $k\{(p)\}$ contains $K = \mathbb{Q}(\zeta_{p(p-1)})$, and that $k\{(p)\}/K$ is abelian and unramified. In particular we will see that Scholz's construction gives a subfield of the Hilbert class field of K.

Classically, proofs that certain extensions are unramified were often done by applying Abhyankar's lemma, which gives sufficient conditions for killing tame ramification in extension fields:

LEMMA 2 (Abhyankar's lemma). *Let L_1/K and L_2/K be finite extensions of algebraic number fields, and let $L = L_1L_2$ denote their compositum. For a prime ideal $\mathfrak{P}$ in L, let e_j $(j = 1, 2)$ denote the ramification indices of the prime $\mathfrak{p}_j = \mathfrak{P} \cap L_j$ below $\mathfrak{P}$ in L_j/K. If $e_2 \mid e_1$ and if $\mathfrak{p}_2$ is tamely ramified in L_2/K, then $\mathfrak{P}$ is unramified in L/L_1.*

Abhyankar's lemma can be used to construct unramified extensions quite easily; its disadvantage lies in the fact that it cannot handle wild ramification. We will circumvent this problem by describing the extensions via ideal groups and using basic class field theory. Our main result is the construction of class fields corresponding to various factors of class numbers of certain cyclotomic number fields that have been found over the last fourty years. Such factors have been constructed using

- the analytic class number formula (Metsänkylä [16]);
- the ambiguous class number formula (Watabe [24]);
- Abhyankar's lemma (Cornell [4, 5, 6], Madan [15], Gold & Madan [8]);
- Iwasawa theory (Ozaki [18]);
- Stickelberger's theorem (Schmidt [21]).

REMARKS. 1. The negative solution of the class field tower problem by Golod and Shafarevich implies the existence of number fields with arbitrarily large degree and bounded root discriminant, hence $\liminf_{n\to\infty} E_n/n = 0$ (this follows already from Scholz's results given above). Scholz's original conjecture that $\lim_{n\to\infty} E_n/n = 0$ seems to be still open.

2. The best upper bounds for $\liminf E_n$ used to come from examples due to Martinet, whose records have recently been improved by Hajir and Maire [9, 10].

3. Scholz communicated most of the results in [22] to Hasse in a letter from Aug. 22, 1936 (see [14]). In this letter he wrote he doubted that $E_p = O(p/\log p)$ where p runs through the primes.

4. There are a lot of open questions regarding the behaviour of root discriminants. The following problem is particularly appealing and might well be accessible with the tools we know today. Let us call a group G *metabelian of level m* if the mth derived group $G^{(m)}$ is trivial but $G^{(m-1)} \neq 1$. Also let $\log_r$ denote the rth iterated logarithm, i.e., $\log_0 n = n$, $\log_1 n = \log n$, and $\log_{r+1} n = \log\log_r n$. Ankeny [1] showed that there is a constant

$c > 0$ such that $\log \mathrm{rd}(K) > c \log_m(K : \mathbb{Q})$ for all normal extensions $K/\mathbb{Q}$ whose Galois group G is metabelian of level $m \geq 1$. It seems not to be known whether this is best possible in the following sense: for any $m \geq 1$, does there exist a sequence of metabelian extensions $K/\mathbb{Q}$ of level m such that $\log \mathrm{rd}(K) = O(\log_m(K : \mathbb{Q}))$? The answer to this question is clearly positive for $m = 1$, where the abelian extensions $K = \mathbb{Q}(\zeta_p)$ satisfy

$$\log \mathrm{rd}(K) = \frac{p-2}{p-1} \log p < \log(K : \mathbb{Q}).$$

Scholz's results imply that the answer is also positive for $m = 2$ since $\log \mathrm{rd}(K) < 2 \log_2(K : \mathbb{Q})$ for the metabelian extensions he constructed.

10. Scholz's construction. We start by introducing the notation and by explaining the relevant facts from class field theory (based on Hasse's exposition [11]). Let k be a number field; a *modulus* is the symbolic product of an integral ideal $\mathfrak{m}$ in $\mathcal{O}_k$ and various real places; the product of all real places of k is denoted by ∞. For infinite places $\mathfrak{p}$, the congruence $\alpha \equiv 1 \bmod \mathfrak{p}$ means that $\sigma(\alpha) > 0$ for the real embedding $\sigma : k \hookrightarrow \mathbb{R}$ corresponding to $\mathfrak{p}$.

Below, we will construct ray class fields modulo $\mathfrak{m} = m\mathcal{O}_k$; to this end, we need a few definitions:

- D_k is the group of fractional ideals in k;
- $D_\mathfrak{m} = \{\mathfrak{a} \in D_k : (\mathfrak{a}, \mathfrak{m}) = 1\}$ is the group of ideals $\mathfrak{a}$ coprime to $\mathfrak{m}$;
- $H_\mathfrak{m} = \{\mathfrak{a} \in D_\mathfrak{m} : \mathfrak{a} = (\alpha)\}$ is its subgroup of principal ideals;
- $H^1_\mathfrak{m} = \{\mathfrak{a} \in D_\mathfrak{m} : \mathfrak{a} = (\alpha), \alpha \equiv 1 \bmod \mathfrak{m}\}$ is the ray mod $\mathfrak{m}$;
- $\mathcal{H} = \{\mathfrak{a} \in D_\mathfrak{m} : N_{k/\mathbb{Q}}\mathfrak{a} = (a),\ a > 0,\ a \equiv 1 \bmod m\}$;
- $E = E_k = \mathcal{O}_k^\times$ is the unit group of $\mathcal{O}_k$;
- $E^1_\mathfrak{m} = \{\eta \in E : \eta \equiv 1 \bmod \mathfrak{m}\}$.

To every ideal group H_F with $H^1_\mathfrak{m} \subseteq H_F \subseteq D_\mathfrak{m}$ class field theory associates a unique abelian extension F/k unramified outside $\mathfrak{m}$. The class field corresponding to the ideal group $H^1_\mathfrak{m}$ is called the *ray class field* of k modulo $\mathfrak{m}$ and will be denoted by $k\{\mathfrak{m}\}$; the extension $k\{\mathfrak{m}\}/k$ is unramified outside m and abelian with Galois group $\mathrm{Gal}(k\{\mathfrak{m}\}/k) \simeq D_\mathfrak{m}/H^1_\mathfrak{m}$. The Artin isomorphism shows that $\mathrm{Gal}(F/k) \simeq D_\mathfrak{m}/H_F$, and Galois theory then gives $\mathrm{Gal}(k\{\mathfrak{m}\}/F) \simeq H_F/H^1_\mathfrak{m}$.

The following result will be of central importance for our construction:

THEOREM 8 (Translation Theorem). *If F is the class field of k to the ideal group H_F defined in k, and if K/k is a finite extension, then FK is the class field of K to the ideal group*

$$\mathcal{T}_K(H_F) = \{\mathfrak{A} \in D_\mathfrak{m}(K) : N_{K/k}\mathfrak{A} \in H_F\}$$

of all ideals $\mathfrak{A}$ in K coprime to $\mathfrak{m}$ such that $N_{K/k}\mathfrak{A}$ is an ideal in H_F.

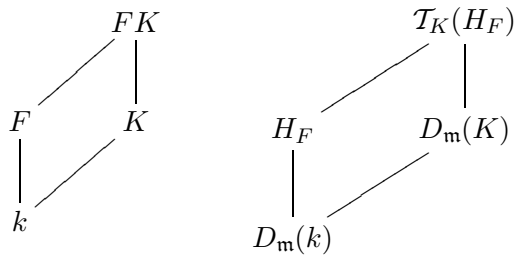

Fig. 1. Translation theorem

The translation theorem immediately yields

LEMMA 3. *The class field of k belonging to the class group $\mathcal{H}$ is the cyclotomic extension $k(\zeta_m)/k$.*

Since the ideal group attached to the Hilbert class field k^1/k is the group $H_{\mathfrak{m}}$ of principal ideals defined mod $\mathfrak{m}$ (here we use the common identification of ideal groups explained in [11]), and since the intersection of ideal groups corresponds to the composita of the class fields, we find the ideal groups attached to the intermediate fields of K/k displayed in Fig. 2.

LEMMA 4. *Let L be the class field of K corresponding to the ideal group H defined mod $\mathfrak{m}$. Then the maximal unramified subextension of L is the class field for the ideal group $H \cdot H_{\mathfrak{m}}$, where $H_{\mathfrak{m}}$ is the ideal group in K consisting of principal ideals coprime to $\mathfrak{m}$. In particular, L is unramified over K if and only if $H_{\mathfrak{m}} \subseteq H$.*

Proof. The maximal unramified subextension of L is the intersection $L \cap K^1$ of L with the Hilbert class field K^1 of K; its associated ideal group is therefore the product of the ideal groups H attached to L and $H_{\mathfrak{m}}$ attached to K^1.

Next, L/K is unramified if and only if $L \subseteq K^1$, that is, if and only if $H \cdot H_{\mathfrak{m}} = H$; the claim now follows. ∎

We also need to explain what we mean by the relative class group. Let K/k be an extension of number fields; the relative norm $N_{K/k}$ maps $\mathrm{Cl}(K)$ to $\mathrm{Cl}(k)$, and its kernel $\mathrm{Cl}(K/k)$ is called the *relative class group* of K/k. If K is a CM-field with maximal real subfield K^+, then we put $\mathrm{Cl}^-(K) = \mathrm{Cl}(K/K^+)$. Finally, if L/K is an extension of CM-fields, then we define $\mathrm{Cl}^-(L/K)$ to be the intersection of the kernels of the norm maps $N_{L/K} : \mathrm{Cl}(L) \to \mathrm{Cl}(K)$ and $N_{L/L^+} : \mathrm{Cl}(L) \to \mathrm{Cl}(L^+)$.

REMARK. There is a second group measuring the "new class group" of K/k (which will play no role here), namely the quotient $\mathrm{Cl}^*(K/k) = \mathrm{Cl}(K)/\mathrm{Cl}(k)^j$, where $\mathrm{Cl}(k)^j$ is the image of the transfer homomorphism $j : \mathrm{Cl}(k) \to \mathrm{Cl}(K)$.

Now we can state our main theorem:

THEOREM 9. *Let k be a totally complex number field of degree $(k:\mathbb{Q})=n$, and let p be a prime that splits completely in $k/\mathbb{Q}$. Assume that $m=p^f>2$, put $\mathfrak{m}=m\mathcal{O}_k$, and let w denote the number of roots of unity contained in k. Let $M=\mathbb{Q}(\zeta_m)$, $F=kM=k(\zeta_m)$, and $K=k^1(\zeta_m)$, where k^1 denotes the Hilbert class field of k (see the Hasse diagram in Fig. 2). Then $k\{\mathfrak{m}\}$ is an unramified abelian extension of F containing K, with relative degree*

$$(k\{\mathfrak{m}\}:F)=\frac{1}{w}\,h(k)\phi(m)^{n/2}(E^1_{\mathfrak{m}}:E^{\phi(m)}). \tag{1}$$

Moreover, the relative class group $\mathrm{Cl}(F/k)$ contains a subgroup C of type

$$C\simeq\mathbb{Z}/\tfrac{\phi(m)}{w}\times(\mathbb{Z}/\phi(m))^{n/2-1}.$$

If k is a CM field, then so is F, and $\mathrm{Cl}^-(F/k)$ contains a subgroup of type C.

Proof. The proof is quite involved, so let us outline the main ideas first. We show that $F=k(\zeta_m)$ is contained in the ray class field $k\{\mathfrak{m}\}$, and that $k\{\mathfrak{m}\}/F$ is unramified. Using the translation theorem, we can transfer the ideal groups attached to $k\{\mathfrak{m}\}/F$ to F, where they are still defined mod $\mathfrak{m}$. Since $k\{\mathfrak{m}\}/F$ is unramified, they can be identified with ideal groups defined mod (1). Finally, we observe that these ideal groups are killed by various relative norms.

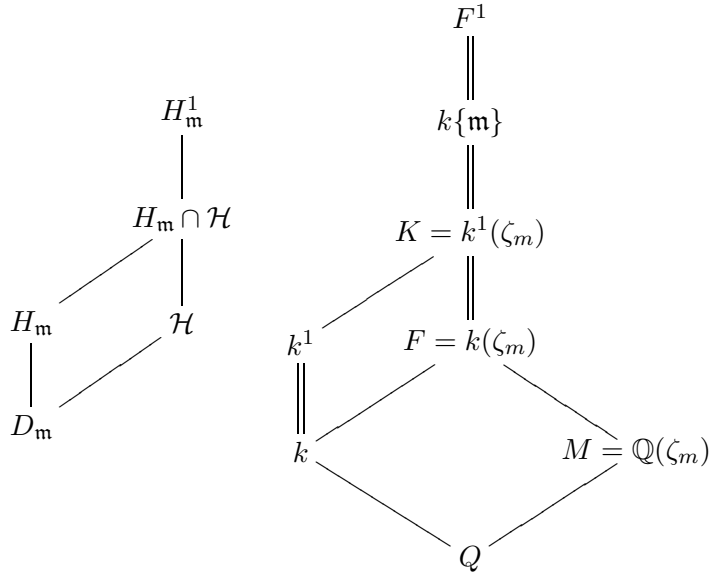

Fig. 2. Ideal groups and fields occurring in the proof of Theorem 9. A $\|$ in the diagram indicates that the corresponding extension is unramified.

1. *F is contained in $k\{\mathfrak{m}\}$.* This follows if we can show that the ideal group $H^1_{\mathfrak{m}}$ attached to $k\{\mathfrak{m}\}$ is contained in the ideal group $\mathcal{H}$ attached to F.

The ideal group corresponding to the class field $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$ is $\{(a) : a \in \mathbb{Z}, a > 0, a \equiv 1 \bmod m\}$. By the translation theorem, this implies that F is the class field for $\mathcal{H}_1 = \{\mathfrak{a} \in D_{\mathfrak{m}}(k) : N_{k/\mathbb{Q}}\mathfrak{a} = (a), a > 0, a \equiv 1 \bmod m\}$. Identifying it with the corresponding group $\mathcal{H} = \mathcal{H}_1 \cap D_{\mathfrak{m}}$, we see that F is the class field for the ideal group $\mathcal{H} : \{\mathfrak{a} \in D_{\mathfrak{m}} : N_{k/\mathbb{Q}}\mathfrak{a} = (a), a > 0, a \equiv 1 \bmod m\}$. Now clearly $H^1_{\mathfrak{m}} \subseteq \mathcal{H}$: in fact, if $\mathfrak{a} = (\alpha)$ for $\alpha \equiv 1 \bmod \mathfrak{m}$, then $N_{k/\mathbb{Q}}\mathfrak{a} = (a)$ for $a = N_{k/\mathbb{Q}}\alpha$, and clearly $a > 0$ (since k is totally complex) and $a \equiv 1 \bmod m$ (since $\alpha \equiv 1 \bmod m\mathcal{O}_k$ implies $N_{k/\mathbb{Q}}\alpha \equiv 1 \bmod m$).

2. *$k\{\mathfrak{m}\}/F$ is unramified.* By the translation theorem, $k\{\mathfrak{m}\}$ is the class field for the ideal group

$$H = \{\mathfrak{A} \in D_{\mathfrak{m}}(F) : N_{F/k}\mathfrak{A} = (\alpha), \alpha \equiv 1 \bmod \mathfrak{m}\}.$$

According to Lemma 4, we need to show that H contains the group $H_{\mathfrak{m}}(F)$ of principal ideals coprime to $\mathfrak{m}$.

To this end, let $A \in F^\times$ be an integer coprime to $\mathfrak{m} = (p^f)$. We will show that $N_{F/k}A \equiv 1 \bmod \mathfrak{p}^f$ for every prime $\mathfrak{p}$ in k above p. Since F/k is completely ramified at $\mathfrak{p}$, every $A \in F^\times$ coprime to $\mathfrak{p}$ is congruent mod $\mathfrak{p}$ to an element in the inertia field, and so we have $A \equiv a \bmod \mathfrak{p}$ for some $a \in k$. But $\mathcal{O}_k/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$ since p splits completely in k, and now it is easy to see that we even have $\mathcal{O}_F/\mathfrak{p}^f \simeq \mathbb{Z}/p^f\mathbb{Z}$. Thus we can choose $a \in \mathbb{Z}$ such that $A \equiv a \bmod \mathfrak{p}^f$. Taking norms shows that $N_{F/k}A \equiv a^{(F:k)} = a^{\phi(m)} \equiv 1 \bmod \mathfrak{p}^f$, which is what we needed to prove.

Remark. Let $\xi_m = \zeta_m + \zeta_m^{-1}$ and put $F_0 = k(\xi_m)$; then the extension $k\{\mathfrak{m}\}/F_0$ is abelian, but not unramified. Since $\mathrm{Gal}(F_0/k)$ acts transitively on half of the prime ideals above p in F_0, the compositum of all the inertia subgroups has index ≤ 4 in $\mathrm{Gal}(k\{\mathfrak{m}\}/k)$. This implies that at least a quotient of C by $\mathbb{Z}/2$ already lives in the class groups $\mathrm{Cl}(F_0/k)$ and $\mathrm{Cl}^-(F_0/k)$, respectively.

3. *Computation of $(k\{\mathfrak{m}\} : F)$.* By now we know that the class number of F is divisible by $(k\{\mathfrak{m}\} : F)$; clearly $(k\{\mathfrak{m}\} : F) = (k\{\mathfrak{m}\} : k)/\phi(m)$, so it remains to compute the index $(k\{\mathfrak{m}\} : k)$. The formula for the number of ray classes gives

$$(k\{\mathfrak{m}\} : k) = (D_{\mathfrak{m}} : H^1_{\mathfrak{m}}) = h(k)\Phi_k(\mathfrak{m})/(E : E^1_{\mathfrak{m}}).$$

Now, we have $\Phi_k(\mathfrak{m}) = \prod \Phi_k(\mathfrak{p}_j^f) = \phi(m)^n$; moreover, $E^{\phi(m)} \subseteq E^1_{\mathfrak{m}}$, and $(E : E^{\phi(m)}) = w\phi(m)^{n/2-1}$. In fact, every element of the $\mathbb{Z}$-basis of the unit group E accounts for a factor of $\phi(m)$, and the unit ζ_w contributes a factor w: since p splits completely in k, we deduce that $p \equiv 1 \bmod w$, hence $\zeta_w^{\phi(m)} = 1$. Thus

$$(E : E^1_{\mathfrak{m}}) = (E : E^{\phi(m)})/(E^1_{\mathfrak{m}} : E^{\phi(m)}) = w\phi(m)^{n/2-1}/(E^1_{\mathfrak{m}} : E^{\phi(m)}),$$

and now we find

$$(k\{\mathfrak{m}\} : k) = \frac{1}{w}\, h(k)\phi(m)^{n/2+1}(E^1_{\mathfrak{m}} : E^{\phi(m)}).$$

Dividing through by $(F : k) = \phi(m)$ we get the class number factor (1) in Theorem 9.

4. *C is a subgroup of the ray class group.* Next we are going to realize the group

$$\mathbb{Z}/\tfrac{\phi(m)}{w} \times (\mathbb{Z}/\phi(m))^{n/2-1}$$

as a subgroup of the ray class group $(H_{\mathfrak{m}} \cap \mathcal{H})/H^1_{\mathfrak{m}} \simeq \mathrm{Gal}(k\{\mathfrak{m}\}/F)$. To this end we first formulate the following

LEMMA 5. *Let F/K be an extension of number fields with degree n, and let $\mathfrak{m}$ be an ideal in $\mathcal{O}_K$ such that every prime dividing $\mathfrak{m}$ splits completely in F/K. Then the norm map $N = N_{F/K}$ induces an exact sequence*

$$1 \to ((\mathcal{O}_K/\mathfrak{m})^\times)^{n-1} \to (\mathcal{O}_F/\mathfrak{m})^\times \xrightarrow{N} (\mathcal{O}_K/\mathfrak{m})^\times \to 1.$$

Proof. Write $\mathfrak{m} = \mathfrak{p}^a\mathfrak{n}$ for some ideal $\mathfrak{n}$ prime to $\mathfrak{p}$, and $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}_1 \cdots \mathfrak{P}_r$. Given a residue class $\alpha \bmod \mathfrak{m}$ with $\alpha \in \mathcal{O}_K$, use the Chinese remainder theorem to find a $\beta \in \mathcal{O}_F$ with $\beta \equiv \alpha \bmod \mathfrak{P}_1^a$, $\beta \equiv 1 \bmod \mathfrak{P}_i^a$ for $2 \le i \le r$, and $\beta \equiv 1 \bmod \mathfrak{n}$. Then $N_{F/K}\beta \equiv \alpha \bmod \mathfrak{m}$. This proves that the norm map is onto.

Now for the kernel: since $(\mathcal{O}_F/\mathfrak{m}\mathcal{O}_F)^\times \simeq ((\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times)^n$, and since the image of the map is $(\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times$, it is sufficient to show that a subgroup isomorphic to $((\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times)^{n-1}$ is in the kernel. This is done as follows: first observe that we can write $\mathfrak{m}\mathcal{O}_F$ as a product $\mathfrak{m}\mathcal{O}_F = \mathfrak{m}_1 \cdots \mathfrak{m}_n$ of relatively prime conjugate ideals $\mathfrak{m}_i$ such that $\mathcal{O}_F/\mathfrak{m}_i \simeq \mathcal{O}_K/\mathfrak{m}\mathcal{O}_K$. Now given any $(a_1, \dots, a_{n-1}) \in (\mathcal{O}_F/\mathfrak{m}_1)^\times \times \cdots \times (\mathcal{O}_F/\mathfrak{m}_{n-1})^\times$, choose algebraic integers $\alpha_1, \dots, \alpha_{n-1} \in \mathcal{O}_F$ such that $\alpha_j \equiv a_j \bmod \mathfrak{m}_j$ and $\alpha_j \equiv 1 \bmod \mathfrak{m}_i$ for every $i \ne j$. Now pick $\alpha_n \in \mathcal{O}_F$ such that $\prod_{j=1}^n \alpha_j \equiv 1 \bmod \mathfrak{m}_n$ and $\alpha_n \equiv 1 \bmod \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}$. Clearly, the α_n are in the kernel of the norm map, and different vectors $(a_1, \dots, a_{n-1})$ give different residue classes $\alpha_n \bmod \mathfrak{m}$. This concludes the proof. ∎

The map sending $\alpha + \mathfrak{m} \in (\mathcal{O}_k/\mathfrak{m})^\times$ to the coset $(\alpha)H^1_{\mathfrak{m}} \in H_{\mathfrak{m}}/H^1_{\mathfrak{m}}$ induces the familiar exact sequence in the first row of the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & E/E^1_{\mathfrak{m}} & \longrightarrow & (\mathcal{O}_k/\mathfrak{m})^\times & \longrightarrow & H_{\mathfrak{m}}/H^1_{\mathfrak{m}} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle N_{k/\mathbb{Q}}} & & \downarrow{\scriptstyle N_{k/\mathbb{Q}}} & & \downarrow{\scriptstyle N_{k/\mathbb{Q}}} & & \\
 & & 1 & \longrightarrow & (\mathbb{Z}/m)^\times & \longrightarrow & (\mathbb{Z}/m)^\times & \longrightarrow & 1
\end{array}$$

Applying the norm $N_{k/\mathbb{Q}}$ to the groups in the first row we see that $N_{k/\mathbb{Q}}E = 1$ since k is totally complex; moreover, $N_{k/\mathbb{Q}}$ maps $(\mathcal{O}_k/\mathfrak{m})^\times$ to $(\mathbb{Z}/m)^\times$,

and Lemma 5 shows that the kernel $A_{\mathfrak{m}}$ of this map is isomorphic to $(\mathbb{Z}/\phi(m))^{n-1}$.

Finally, $N_{k/\mathbb{Q}}$ maps ideals $(\alpha) \in H_{\mathfrak{m}}$ to ideals $(a) \in H_{m\infty}$; thus we get a map $N_{k/\mathbb{Q}} : H_{\mathfrak{m}}/H^1_{\mathfrak{m}} \to H_{m\infty}/H^1_{m\infty}$ whose kernel consists of all elements $(\alpha)H^1_{\mathfrak{m}}$ such that $N_{k/\mathbb{Q}}(\alpha) = (a)$ for $a \equiv 1 \bmod m\infty$. This immediately shows that the kernel is just the ideal group $\mathcal{H} \cap H_{\mathfrak{m}}/H^1_{\mathfrak{m}}$. The group $H_{m\infty}/H^1_{m\infty}$ is the ray class group in $\mathbb{Q}$ attached to the cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ and is thus isomorphic to $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m)^\times$; this can, of course, also be checked directly by sending an ideal $(a) \in H_{m\infty}$ with $a > 0$ to its residue class $a + m\mathbb{Z}$.

The snake lemma then provides us with the exact sequence

$$1 \to E/E^1_{\mathfrak{m}} \to A_{\mathfrak{m}} \to \mathcal{H} \cap H_{\mathfrak{m}}/H^1_{\mathfrak{m}} \to 1. \tag{2}$$

Clearly $E/E^1_{\mathfrak{m}}$ is a factor group of $E/E^{\phi(m)} \simeq \mathbb{Z}/w \times (\mathbb{Z}/\phi(m))^{n/2-1}$; this shows that $\mathcal{H} \cap H_{\mathfrak{m}}/H^1_{\mathfrak{m}}$ contains a subgroup $\mathcal{C}/H^1_{\mathfrak{m}} \simeq C = \mathbb{Z}/\frac{\phi(m)}{w} \times (\mathbb{Z}/\phi(m))^{n/2-1}$ as claimed.

5. *C is a subgroup of* $\mathrm{Cl}(F/k)$. We now use the translation theorem to lift the ideal groups attached to K and $k\{\mathfrak{m}\}$ from k to F, where the groups will have conductor 1 since the extensions are unramified.

(1) $\mathcal{T}(\mathcal{H}) = D_{\mathfrak{m}}(F)$.
(2) $\mathcal{T}(H_{\mathfrak{m}} \cap \mathcal{H}) = \mathcal{T}(H_{\mathfrak{m}}) = \{\mathfrak{A} \in D_{\mathfrak{m}}(F) : N_{F/k}\mathfrak{A} = (\alpha)\}$.
(3) $\mathcal{T}(H^1_{\mathfrak{m}}) = \{\mathfrak{A} \in D_{\mathfrak{m}}(F) : N_{F/k}\mathfrak{A} \in H^1_{\mathfrak{m}}\}$.

Since we know that the class field of $\mathcal{T}(H_{\mathfrak{m}})$ is unramified, it follows that it can be identified with an ideal group I_F defined modulo (1); recall that $\mathcal{T}(H_{\mathfrak{m}})$ is the group you get by omitting all ideals not coprime to $\mathfrak{m}$ from I_F. Since applying the relative norm $N_{F/k}$ to the ideals in I_F gives principal ideals, it is immediately clear that the corresponding class group I_F/H_F is contained in the relative class group $\mathrm{Cl}(F/k)$.

6. *C is a subgroup of the minus class group.* Assume that k is a CM-field, and let $\nu = N_{k/k^+}$ denote the relative norm from k to its maximal real subfield k^+. Consider the ideal group $\mathcal{H}^+ = \{\mathfrak{a} \in D_m : \mathfrak{a} = (\alpha), \nu\alpha \equiv 1 \bmod m\}$. We claim that there is an exact sequence

$$1 \to W_k \to (\mathcal{O}/\mathfrak{m})^\times[\nu] \xrightarrow{\omega} \mathcal{H}^+/H^1_{\mathfrak{m}} \to 1,$$

where $(\mathcal{O}/\mathfrak{m})^\times[\nu]$ is the subgroup of $(\mathcal{O}/\mathfrak{m})^\times$ killed by ν.

The homomorphism $\omega : (\mathcal{O}/\mathfrak{m})^\times[\nu] \to \mathcal{H}^+; \alpha + \mathfrak{m} \mapsto (\alpha)$ is surjective by definition, and its kernel consists of all residue classes $\alpha + \mathfrak{m}$ with $(\alpha) = (1)$ and $\nu\alpha \equiv 1 \bmod m$. The only unit in k^+ congruent to 1 mod m is 1, hence the kernel consists of all $\alpha + \mathfrak{m}$ for which α is a unit in $\mathcal{O}_k^\times$ with relative

norm 1. The only such units are the roots of unity, and this shows that $\ker\omega$ is just the image of W_k in $(\mathcal{O}/\mathfrak{m})^\times$.

From Lemma 5 we get $(\mathcal{O}/\mathfrak{m})^\times[\nu] \simeq (\mathcal{O}_{k^+}/(m))^\times \simeq ((\mathbb{Z}/m)^\times)^{n/2}$, and this implies $\mathcal{H}^+/H^1_{\mathfrak{m}} \simeq C$.

Lifting $\mathcal{H}^+$ to an ideal group $\mathcal{T}(\mathcal{H}^+)$ defined in F, we get a subgroup of the group of ideals in F that is killed by the relative norm N_{F/F^+}. Thus $\mathrm{Cl}^-(F)$ contains a subgroup of type C. Since this subgroup is also contained in $\mathrm{Cl}(F/k)$, we deduce that $\mathrm{Cl}^-(F/k)$ contains a subgroup of type C, and this concludes the proof of Theorem 9. ∎

Example. Consider the field $K = \mathbb{Q}(\zeta_{155})$. If we take $m = 31$ and $k = \mathbb{Q}(\zeta_5)$, then we find that $\mathrm{Cl}^-(K/k)$ contains a subgroup of type $\mathbb{Z}/3 \times \mathbb{Z}/30$. If we take the subfield of degree 10 of $\mathbb{Q}(\zeta_{31})$ as k and $m = 5$, then we find the subgroup $\mathbb{Z}/2 \times (\mathbb{Z}/4)^4$ of $\mathrm{Cl}^-(F/k)$, where $F = k(\zeta_5)$.

11. Applications. Here we will derive a couple of corollaries from our result. To this end we need the following observation:

Lemma 6. *Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic number field with $n \not\equiv 2 \bmod 4$, and let p be a prime. Then the number w of roots of unity contained in the decomposition field k of p in $K/\mathbb{Q}$ is given by*

$$w = \begin{cases} 2 & \text{if } p = 2, \\ (p-1, n) & \text{if } p > 3 \text{ and } 2 \mid n, \\ (p-1, 2n) & \text{if } p > 3 \text{ and } 2 \nmid n. \end{cases} \tag{3}$$

Proof. Let us dispose of the case $p = 2$ first: if p splits completely in a field containing ζ_w with $w > 2$, then we must have $p \equiv 1 \bmod w$: contradiction. Thus $w = 2$ if $p = 2$.

Now assume that p is odd; the same argument as above shows that $w \mid p-1$. Moreover, since $k \subseteq K$ we clearly have $w \mid n$ or $w \mid 2n$ according as n is even or odd. Thus $w \mid (p-1, n)$ if n is even and $w \mid (p-1, 2n)$ if n is odd. Conversely, if n is even and $w \mid (p-1, n)$, then p splits in $\mathbb{Q}(\zeta_w)$ and $\mathbb{Q}(\zeta_w) \subseteq K$, hence $\zeta_w \in k$. The argument for n odd is similar. ∎

This allows us to reformulate Theorem 9 somewhat:

Corollary 1. *Let $n \not\equiv 2 \bmod 4$ be an integer, p a prime not dividing n, and assume that there is no integer j such that $p^j \equiv -1 \bmod n$. Let k be the decomposition field of p in $\mathbb{Q}(\zeta_n)$; then the relative minus class group $\mathrm{Cl}^-(K/k)$ of $K = k(\zeta_{p^f})$ contains a subgroup of type $\mathbb{Z}/\frac{u}{w} \times (\mathbb{Z}/u)^{e/2-1}$, where $u = \phi(p^f)$, w is defined as in Lemma 6, and $e = \phi(n)/o_n(p)$, where $o_n(p)$ denotes the order of p modulo n.*

Proof. The condition $p^j \not\equiv -1 \bmod n$ is equivalent to the decomposition field k of p in $\mathbb{Q}(\zeta_n)$ being complex; we apply Theorem 9 to $k(\zeta_n)/k$ and

observe that $(k : \mathbb{Q}) = \phi(n)/o_n(p)$ and that k contains the wth roots of unity. ∎

As another corollary we get a result due to B. Schmidt [21, Thm. 3.3]; he calls a prime p *self-conjugate modulo* $m = p^a n$ if there is an integer j such that $p^j \equiv -1 \bmod n$.

COROLLARY 2. *Assume that p is not self-conjugate modulo $m = p^a n$. Then the minus class group $\mathrm{Cl}^-(K)$ of $K = \mathbb{Q}(\zeta_m)$ has a subgroup of type*

$$(\mathbb{Z}/w_0\mathbb{Z}) \times (\mathbb{Z}/\phi(p^a)\mathbb{Z})^{e/2-1},$$

where $e = \phi(n)/o_n(p)$, $w_0 = \phi(p^a)/w$, and w is defined by (3).

Proof. This follows at once from Corollary 1. ∎

Here is another application of our result:

PROPOSITION 14. *Let p be an odd prime, $L = \mathbb{Q}(\zeta_{4p^2})$, and let K be the cyclic extension of degree p over $k = \mathbb{Q}(\zeta_4)$ contained in L. Then $p \mid h^-(K)$ if $p \equiv 1 \bmod 4$ and $p \nmid h(K)$ if $p \equiv 3 \bmod 4$.*

Proof. It follows from Theorem 9 that $p \mid h^-(K)$ if $p \equiv 1 \bmod 4$, so assume that $p \equiv 3 \bmod 4$. Then only the prime ideal p ramifies in K/k, and the ambiguous class number formula shows $p \nmid h(K)$. ∎

Using the same proof, we can show

PROPOSITION 15. *Let $p \equiv 1 \bmod 4$ be prime, and let $\mathfrak{p}$ denote a prime ideal in $k = \mathbb{Q}(i)$ above p. Then there exists a $\mathbb{Z}_p$-extension k_∞/k which is unramified outside $\mathfrak{p}$; moreover, $k_\infty K_\infty$ is an unramified $\mathbb{Z}_p$-extension of the cyclotomic $\mathbb{Z}_p$-extension K_∞ of k.*

It is also possible to prove this by applying the "blowing up" results from [13] to the results of Proposition 14; one immediately sees that the class group of the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of K has a subgroup isomorphic to $\mathbb{Z}/p^{n+1}\mathbb{Z}$ if $p \equiv 1 \bmod 4$.

Metsänkylä's factorization revisited. In [12], we derived the following factorization of the class number of certain CM-fields due to Metsänkylä [16]:

PROPOSITION 16. *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.

Assume that $L = \mathbb{Q}(\zeta_{pq})$ with $p \equiv 1 \bmod q$; by what we have shown, $\mathrm{Cl}^-(L)$ contains a subgroup of type $C = \mathbb{Z}/\frac{p-1}{2} \times (\mathbb{Z}/p-1)^{(q-3)/2}$. Is this a factor of T_2? The Remark at the end of item 2 in the proof of Theorem 9 shows that $\mathrm{Cl}^-(L_2L_1^+/L_2)$ contains at least a quotient of C by $\mathbb{Z}/2\mathbb{Z}$.

REMARKS. Let me add a few remarks concerning [12]. [12, Prop. 2], which I credited to Louboutin, actually already appears as Proposition 3 in [25]. Also, Schoof [23] introduced a unit index $[\mu_K : \mu_K^-]$ which coincides with $2/Q^*$ in Hasse's work.

Acknowledgements. I thank the referee for reading the manuscript very carefully.

References

[1] N. C. Ankeny, *An improvement of an inequality of Minkowski*, Proc. Nat. Acad. Sci. U.S.A. 37 (1951), 711–716.

[2] H. F. Blichfeldt, *A new upper bound to the minimum value of the sum of linear homogeneous forms*, Monatsh. Math. Phys. 43 (1936), 410–414.

[3] —, *Note on the minimum value of the discriminant of an algebraic field*, ibid. 48 (1939), 531–533.

[4] G. Cornell, *Abhyankar's lemma and the class group*, in: Number Theory Carbondale, Lecture Notes in Math. 751, Springer, 1971, 82–88.

[5] —, *On the construction of relative genus fields*, Trans. Amer. Math. Soc. 271 (1982), 501–511.

[6] —, *Relative genus theory and the class group of l-extensions*, ibid. 277 (1983), 421–429.

[7] G. Cornell and M. Rosen, *The ℓ-rank of the real class group of cyclotomic fields*, Compos. Math. 53 (1984), 133–141.

[8] R. Gold and M. L. Madan, *Some applications of Abhyankar's lemma*, Math. Nachr. 82 (1978), 115–119.

[9] F. Hajir and C. Maire, *Tamely ramified towers and discriminant bounds for number fields*, Compos. Math. 128 (2001), 35–53.

[10] —, —, *Tamely ramified towers and discriminant bounds for number fields. II*, J. Symbolic Comput. 33 (2002), 415–423.

[11] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I*: *Klassenkörpertheorie*, Jahresber. Deutsch. Math.-Verein. 35 (1926), 1–55.

[12] F. Lemmermeyer, *Ideal class groups of cyclotomic number fields I*, Acta Arith. 72 (1995), 347–359.

[13] —, *Ideal class groups of cyclotomic number fields II*, ibid. 84 (1998), 59–70.

[14] F. Lemmermeyer (ed.), *Der Briefwechsel H. Hasse — A. Scholz*, in preparation.

[15] M. L. Madan, *Class groups of global fields*, J. Reine Angew. Math. 252 (1972), 171–177.

[16] T. Metsänkylä, *Über den ersten Faktor der Klassenzahl des Kreiskörpers*, Ann. Acad. Sci. Fenn. Ser. A I 416 (1967), 7–48.

[17] N. Nakagoshi, *A construction of unramified abelian l-extensions of regular Kummer extensions*, Acta Arith. 44 (1984), 47–58.

[18] M. Ozaki, *On the p-rank of the ideal class group of the maximal real subfield of a cyclotomic field*, preprint 1997; now published as *An application of Iwasawa theory to constructing fields $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ which have class group with large p-rank*, Nagoya Math. J. 169 (2003), 179–190.

[19] C. A. Rogers, *The product of n homogeneous linear forms*, J. London Math. Soc. 24 (1949), 31–39.
[20] —, *The product of n real homogeneous linear forms*, Acta Math. 82 (1950), 185–208.
[21] B. Schmidt, *Cyclotomic integers of prescribed absolute value and the class group*, J. Number Theory 72 (1998), 269–281.
[22] A. Scholz, *Minimaldiskriminanten algebraischer Zahlkörper*, J. Reine Angew. Math. 179 (1938), 16–21.
[23] R. Schoof, *Minus class groups of the fields of the lth roots of unity*, Math. Comp. 67 (1998), 1225–1245.
[24] M. Watabe, *On class numbers of some cyclotomic fields*, J. Reine Angew. Math. 301 (1978), 212–215.
[25] K. Yoshino and M. Hirabayashi, *On the relative class number of the imaginary abelian number field. I. II*, Mem. Coll. Liberal Arts Kanazawa Medical Univ. 9 (1981), 5–53; ibid. 10 (1982), 33–81.

Mörikeweg 1
73489 Jagstzell, Germany
E-mail: hb3@ix.urz.uni-heidelberg.de

Received on 14.6.2007
and in revised form on 2.11.2007 (5462)