ACTA ARITHMETICA
LXXXIV.1 (1998)

Ideal class groups of cyclotomic number fields II

by

Franz Lemmermeyer (Saarbrücken)

This is a continuation of [13]; parts I and II are independent, but will be used in part III.

5. The 2-class group. Let $h(m)$ and $h^+(m)$ denote the class number of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m+\zeta_m^{-1})$, respectively, and put $h^-(m) = h(m)/h^+(m)$. In this section we will show how the results on the 2-class field tower of quadratic number fields can be used to improve the results of Stevenhagen [30] on the parity of $h^+(m)$ for certain composite m with few prime factors.

Proposition 4. *Let $p \equiv q \equiv 1 \bmod 4$ be primes, put $L = \mathbb{Q}(\zeta_{pq})$, and let K and K^+ be the maximal 2-extensions contained in L and $L^+ = L \cap \mathbb{R}$, respectively.*

1. *$2 \mid h(K^+)$ if and only if $(p/q) = 1$;*
2. *if $(p/q) = 1$ and $(p/q)_4 = (q/p)_4$, then $2 \mid h(F)$ for every subfield $F \subseteq L$ containing $\mathbb{Q}(\sqrt{pq}\,)$;*
3. *if $(p/q)_4 = (q/p)_4 = +1$, then $4 \mid h(K^+)$.*

P r o o f. By a result of Rédei and Reichardt [23, 24], the quadratic number field $k = \mathbb{Q}(\sqrt{pq}\,)$ admits a cyclic quartic extension F/k which is unramified outside ∞ and which is normal over $\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) \simeq D_4$, the dihedral group of order 8. The last property guarantees that F is either totally real or totally complex; Scholz [26] has shown that F is real if and only if $(p/q)_4 = (q/p)_4$.

Assume that F is real; then, for every subfield M of K^+ containing $\mathbb{Q}(\sqrt{pq}\,)$, the extension FK^+/K^+ is unramified everywhere and is cyclic of degree 2 (if $\mathbb{Q}(\sqrt{p}, \sqrt{q}\,) \subseteq M$) or 4 (otherwise); by Hilbert's theorem 94 this implies that the class number of M is even.

If F is totally complex, we consider the field K^+. In this case, K and FK^+ are totally complex quadratic extensions of K^+ which are unramified

1991 *Mathematics Subject Classification*: Primary 11R21; Secondary 11R29, 11R18.

at the finite primes. Let N be the quadratic subextension of FK/K^+ different from K and FK^+. Then N is totally real and unramified at the finite primes, and we see that K^+ has even class number.

Finally, if $(p/q)_4 = (q/p)_4 = +1$, then k admits a cyclic octic extension which is unramified outside ∞ and normal over $\mathbb{Q}$; the same proof as above shows that $4 \mid h(K^+)$.

The fact that K^+ has odd class number if $(p/q) = -1$ is given as Exercise 10.4 in [32]; here is a short proof: since only p ramifies in the 2-extension $K_p^+/\mathbb{Q}$, Theorem 10.4 in [32] (this is a very special case of the ambiguous class number formula) says that K_p^+ has odd class number. Now $K_p^+/\mathbb{Q}$ is cyclic, and $\mathbb{Q}(\sqrt{p}\,)$ is its unique quadratic subfield. Since q is inert in $\mathbb{Q}(\sqrt{p}\,)$, we conclude that $\mathbb{Q}$ must be the decomposition field of q, i.e. q is inert in $K_p^+/\mathbb{Q}$. Thus q is the only ramifying prime in K_{pq}^+/K_p^+, and again Theorem 10.4 proves our claim.

The fact that $h_2(K^+) = 1$ if $(p/q) = -1$ also follows from a result of Milgram [19] and the class number formula. ∎

The idea behind this proof can be found in van der Linden's paper [15]. Our next result strengthens a result of Cornell and Washington [3], who showed that $h^+(m)$ is even if m is divisible by at least four primes $\equiv 1 \bmod 4$:

Proposition 5. *Let m be an integer divisible by three distinct primes $\equiv 1 \bmod 4$; then $2 \mid h^+(m)$.*

Proof. It is sufficient to prove the claim for $m = p_1p_2p_3$, where the $p_j \equiv 1 \bmod 4$ are pairwise distinct primes (this follows from the fact that $h^+(m) \mid h^+(mn)$, which is true by class field theory, since the maximal real subfield of $\mathbb{Q}(\zeta_m)$ does not have unramified quadratic extensions inside the maximal real subfield of $\mathbb{Q}(\zeta_{mn})$).

If two of them are quadratic residues of each other, then the claim follows from Proposition 4.

If $(p_1/p_2) = (p_2/p_3) = (p_3/p_1) = -1$, then there exists an unramified quaternion extension L of $\mathbb{Q}(\sqrt{m}\,)$, which is normal over $\mathbb{Q}$ (see [14]). In particular, L is either totally real or totally complex.

If it is totally real, then the extension LK^+/K^+ is unramified (where $K = \mathbb{Q}(\zeta_m)$ and K^+ is its maximal real subfield).

If L is totally complex, then K/K^+ and KL/K^+ are two different CM-extensions of K^+ which are unramified outside ∞; the quadratic subextension of KL/K^+ different from K and L is a totally real quadratic unramified extension of K^+. This proves the claim. ∎

Yet another application of this trick is

Proposition 6. *Let $p \equiv -q \equiv -q' \equiv 1 \bmod 4$ be primes such that $(p/q) = (p/q') = 1$. Then $2 \mid h^+(pqq')$.*

P r o o f. Consider the quadratic number field $\mathbb{Q}(\sqrt{-pq}\,)$; since $(p/q) = 1$, it has class number divisible by 4, and the results of Rédei and Reichardt show that the 4-class field of k is generated by the square root of $\alpha_q = x + y\sqrt{p}$, where $x, y \in \mathbb{Z}$ satisfy $x^2 - py^2 = -qz^2$; the same is true with q replaced by q'. Since both α_q and $\alpha_{q'}$ have mixed signature, their product is either totally positive or totally negative. The rest of the proof is clear. ∎

REMARK. Any of the primes $p \equiv 1 \bmod 4$ in the propositions above may be replaced by $p = 8$. Note that $(q/8)_4$ is defined by $(q/8)_4 = (-1)^{(q-1)/8}$ for all primes $q \equiv 1 \bmod 8$.

6. Morishima's results. In this section we will generalize a result about the 2-class group of certain cyclotomic fields first proved by Morishima in [20]. There he also proved a result about capitulation in cyclic unramified extensions of relative degree p, which we will give in the next section, along with related results which will be useful in Section 8.

THEOREM 4. *Let k^+ be a totally real number field, and let $\mathfrak{p}$ be a principal prime ideal k^+. Assume that the class number of k^+ is divisible by some integer n, and let K^+/k^+ be a cyclic unramified extension of relative degree n. Let k be a totally complex quadratic extension of k^+ in which $\mathfrak{p}$ is ramified, and put $K = kK^+$. Then $\mathrm{Cl}(K)$ contains a subgroup of type $(\mathbb{Z}/2\mathbb{Z})^{n-1}$.*

P r o o f. We use a lower bound for the rank of the relative class group

$$\mathrm{Cl}_p(K/k) = \ker(N : \mathrm{Cl}_p(K) \to \mathrm{Cl}_p(k))$$

due to Jehne [11], who showed that, for cyclic extensions K/k of prime degree p, we have

$$\operatorname{rank} \mathrm{Cl}_p(K/k) \geq \#\,\mathrm{Ram}(K/k) - \operatorname{rank}_p E_k/H - 1. \tag{1}$$

Here $\mathrm{Ram}(K/k)$ denotes the set of (finite and infinite) primes of k ramified in K, and $H = E_k \cap NK^\times$ is the subgroup of units which are norms of elements (or equivalently, by Hasse's norm theorem, which are local norms).

Applying this to the quadratic extension K/k^+, we see that $\mathrm{Ram}(K/K^+)$ contains n primes above $\mathfrak{p}$, as well as the $(K^+ : \mathbb{Q})$ infinite primes; moreover, H contains E^2 (where $E = E_{K^+}$), hence $(E : H) \mid (E : E^2) = (K^+ : \mathbb{Q})$, and Jehne's estimate gives $\operatorname{rank} \mathrm{Cl}_2(K/K^+) \geq n - 1$. ∎

COROLLARY 1. *Let k be a complex subfield of $\mathbb{Q}(\zeta_p)$, let K^+ be an abelian unramified extension of k^+ of degree n, and put $K = kK^+$. Then $\mathrm{Cl}_2(K)$ contains a subgroup of type $(\mathbb{Z}/2\mathbb{Z})^{n-1}$.*

P r o o f. Observe that the prime ideal above p in k^+ is principal (it is the relative norm of $1 - \zeta_p$), and apply Theorem 4. ∎

Although this result might help to explain why class groups of real subfields of cyclotomic fields with small conductor are small, one should not regard it as a support for Vandiver's conjecture that $p \nmid h^+(p)$. Of course, Corollary 1 predicts that $\mathrm{Cl}(K)$ has a subgroup of type $(\mathbb{Z}/2\mathbb{Z})^{p-1}$ in this case (with some $p > 10^6$, since Vandiver's conjecture holds for smaller p), but there is no reason to suspect that this should be impossible for fields with large degree and discriminant. In fact, Cornell and Washington [3] showed that there are cyclotomic fields $\mathbb{Q}(\zeta_p)$ with $h^+(p) > p$, and more recently Jeannin [10] found many quintic cyclic fields with large class number.

EXAMPLE. Let k be the quartic subfield of $\mathbb{Q}(\zeta_{229})$; then $k^+ = \mathbb{Q}(\sqrt{229}\,)$ has class number 3 and Hilbert class field $K^+ = k^+(\alpha)$, where $\alpha^3 - 4\alpha - 1 = 0$. Computations with Pari [1] give $\mathrm{Cl}(K) \simeq \mathbb{Z}/17\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^4$. The subgroup of order 17 comes from $\mathrm{Cl}(k) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$, while Corollary 1 predicts that $\mathrm{Cl}(K)$ contains a subgroup of type $(\mathbb{Z}/2\mathbb{Z})^2$.

The next two corollaries give examples of cyclic quartic fields with infinite class field tower:

COROLLARY 2. *Let $p \equiv 5 \bmod 8$ be a prime; if the class number h of $k = \mathbb{Q}(\sqrt{p}\,)$ is ≥ 15, then the class field tower of the quartic cyclic field K of conductor p is infinite (actually this holds for any complex cyclic quartic field K containing k).*

Proof. Let F be the Hilbert class field of k; by Corollary 1, the compositum KF has a class group of 2-rank $r \ge h - 1$; by the criterion of Golod–Shafarevich, KF has infinite 2-class field tower if

$$r \ge 2 + 2\sqrt{1 + \operatorname{rank} E/E^2} = 2 + 2\sqrt{2h+1}.$$

If $h \ge 14$, this inequality is satisfied, and our claim follows (note that h is odd). ∎

EXAMPLE. If $p = 13693$, then $h = 15$.

COROLLARY 3. *Let $p \equiv q \equiv 1 \bmod 4$ be primes such that $pq \equiv 5 \bmod 8$; assume that the fundamental unit ε of $k = \mathbb{Q}(\sqrt{pq}\,)$ has positive norm, and that $h(k) \ge 6$. Then the two cyclic complex quartic subfields of $\mathbb{Q}(\zeta_p)$ containing k have infinite class field tower.*

Proof. Since ε has positive norm, the prime ideals above p and q are principal. Thus both ideals split in F/k (we use the same terminology as above), and $\mathrm{Ram}(KF/F)$ contains $2n$ prime ideals. This gives $\operatorname{rank} \mathrm{Cl}_2(KF) \ge 2n - 1$, and the bound of Golod–Shafarevich shows that KF has infinite class field tower if $h(k) \ge 5$; since $h(k)$ is even, we actually have $h(k) \ge 6$. ∎

EXAMPLE. (a) If $p = 5$ and $q = 353$, then $h = 6$.

(b) According to Schoof [29], the plus class number of $\mathbb{Q}(\zeta_p)$ for $p = 3547$ equals 16777; this implies that $\mathbb{Q}(\zeta_p)$ has infinite class field tower.

(c) Cornacchia [2] has shown that the cyclic quintic extension of conductor 3931 has 2-class number 2^8; this implies that the subfield of degree 10 in $\mathbb{Q}(\zeta_{3931})$ has infinite 2-class field tower.

Techniques similar to those used in the proof of Theorem 4 were used by Martinet [17], Schmithals [25] and Schoof [27] to construct quadratic number fields with infinite class field towers; note, however, that a related construction by Matsumura [18] is incorrect: the error occurs in his proof of Lemma 4. In fact, here is a counter-example to his Theorem 1: take $p = 17$, $q = -23$, $l = 3$; his Theorem 1 predicts that the compositum K of $\mathbb{Q}(\sqrt{-23}, \sqrt{17})$ and the cubic field of discriminant -23 has an ideal class group with subgroup $(2, 2)$. However, $\mathrm{Cl}(K) \simeq \mathbb{Z}/7\mathbb{Z}$ by direct computation.

Ozaki [22] found an original construction of real abelian fields with large l-class groups; using l-adic L-functions and Iwasawa theory, he proved the following result:

PROPOSITION 7. *There exist abelian extensions $M/\mathbb{Q}$ whose conductor is a product of three different primes, such that* $\operatorname{rank} \mathrm{Cl}_l(M)$ *exceeds any given integer.*

Proof. Fix an odd prime l; for a prime $q \equiv 1 \bmod l$, let k_q denote the subfield of $\mathbb{Q}(\zeta_q)$ of degree l. Choose odd primes p, q and r such that $p \equiv q \equiv 1 \bmod l$, and let n be the largest odd divisor of $r - 1$ such that $p^{(r-1)/n} \equiv q^{(r-1)/n} \equiv 1 \bmod r$. Let K be the subfield of $\mathbb{Q}(\zeta_r)$ with degree n. Then $L = Kk_pk_q$ is a normal extension of K with $\mathrm{Gal}(L/K) \simeq (l, l)$, and the primes p and q split completely in $K/\mathbb{Q}$.

Let M be any of the $l - 1$ intermediate fields of L/K different from Kk_p and Kk_q; since these fields have conductor pqr, all the primes above p and q in K (there are exactly $2n$ such primes) must ramify in M/K; since K is real, it does not contain ζ_l, hence $\operatorname{rank}_l E/H \le \operatorname{rank} E/E^l = n-1$, and (1) shows that $\operatorname{rank} \mathrm{Cl}_l(M/K) \ge 2n-(n-1)-1 = n$. Since $(\mathrm{Cl}_l(M) : N_{L/M}\, \mathrm{Cl}_l(L)) = l$ by class field theory, we must have $\operatorname{rank} \mathrm{Cl}_l(M/K) \ge n - 1$.

Since, for given $n \in \mathbb{N}$, there are infinitely many primes $r \equiv 1 \bmod n$ and $p \equiv q \equiv 1 \bmod lr$, our claim follows.

Incidentally, the same argument works if we replace k_p by the field of degree l and conductor l^2. ∎

7. Capitulation of ideal classes. We want to study the following situation: let L/F be an abelian extension with Galois group $G = \mathrm{Gal}(L/F) \simeq \Delta \times \Gamma$, where Δ and Γ are cyclic groups of coprime order. Let k and K denote the fixed fields of Γ and Δ, respectively; then we can identify

$\Delta = \mathrm{Gal}(k/F) \simeq \mathrm{Gal}(L/K)$ and $\Gamma = \mathrm{Gal}(L/k) \simeq \mathrm{Gal}(K/F)$ (see Figure 1 for the Hasse diagrams).

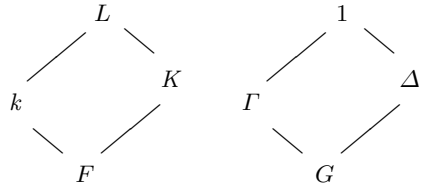

Fig. 1

Let M be a G-module of order coprime to $\#\Delta$ (e.g. $M = \mathrm{Cl}_p(L)$, $\mathrm{Cl}_p(L/k)$, or $\kappa = \kappa_{L/k}$ for primes $p \nmid \#\Delta$); we can decompose M using the idempotents e_ϕ of the group ring $\mathbb{Z}[\Delta]$ as $M = \bigoplus M(\phi)$ with $M(\phi) = e_\phi(M)$. Now we use (cf. Schoof [28])

Proposition 8. *In this notation we have* $\widehat{\mathrm{H}}^q(\Gamma, M)(\phi) \simeq \widehat{\mathrm{H}}^q(\Gamma, M(\phi))$.

Proof. Let $\phi \ne \chi$ be different characters of Δ, and consider the submodule $\widehat{\mathrm{H}}^q(\Gamma, M(\phi))$; then $\widehat{\mathrm{H}}^q(\Gamma, M(\phi))(\chi) = 0$, since e_χ kills the image of every $x \in \widehat{\mathrm{H}}^q(\Gamma, M(\phi))$. Thus the injection $\imath : \widehat{\mathrm{H}}^q(\Gamma, M)(\chi) \hookrightarrow \widehat{\mathrm{H}}^q(\Gamma, M)$ actually lands in $\widehat{\mathrm{H}}^q(\Gamma, M(\chi))$, and we have an injection $\imath : \widehat{\mathrm{H}}^q(\Gamma, M)(\chi) \hookrightarrow \widehat{\mathrm{H}}^q(\Gamma, M(\chi))$. Summing over all inequivalent χ we get $\widehat{\mathrm{H}}^q(\Gamma, M)$ on both sides, hence $\imath$ must be an isomorphism. ∎

Since L/k is cyclic, we have an injection $\kappa \hookrightarrow \widehat{\mathrm{H}}^{-1}(\Gamma, E_L)$ (see Iwasawa [8]); here $\widehat{\mathrm{H}}^q$ denotes Tate's cohomology groups. Taking the ϕ-parts of this injection we find $\kappa(\phi) \hookrightarrow \widehat{\mathrm{H}}^{-1}(\Gamma, E_L)(\phi)$. Now Proposition 8 shows that $\kappa(\phi) \hookrightarrow \widehat{\mathrm{H}}^{-1}(\Gamma, E_L(\phi))$.

As a special case, let L and k be CM-fields with maximal real subfields K and F, respectively (in particular, $\Delta = \{1, J\}$, where J denotes complex conjugation). Then the minus part of $\widehat{\mathrm{H}}^{-1}(\Gamma, E_L)$ is $\widehat{\mathrm{H}}^{-1}(\Gamma, E_L^-) = \widehat{\mathrm{H}}^{-1}(\Gamma, W_L) \simeq {}_N W_L / W_L^{1-\sigma}$, where ${}_N W_L = \{\zeta \in W_L : N_{L/k}\zeta = 1\}$. We have shown (compare Jaulent [9] and Kida [12]):

Proposition 9. *Let L/k be a cyclic extension of CM-fields of odd prime degree p. Then $\kappa_{L/k}^- = \kappa_{L/k} \cap \mathrm{Cl}^-(k)$ is isomorphic to a subgroup of ${}_N W_L / W_L^{1-\sigma}$. In particular, $\#\kappa_{L/k}^- \mid p$.*

Let k be a number field containing a pth root of unity ζ_p. A cyclic extension L/k of degree p is called *essentially ramified* if $L = k(\sqrt[p]{\alpha})$ and $\alpha\mathcal{O}_k$ is not the pth power of an ideal. In particular, subextensions of $k(\sqrt[p]{E_k})/k$ are not essentially ramified. In [12], Kida showed (generalizing results of Moriya [21] and Greenberg [5]) that $\kappa_{L/k}^- = 1$ if $\zeta_p \notin k$, if $L = k(\zeta_{p^n})$ for some

$n \geq 1$, or if L/k is ramified outside p. We will now show that this result is almost best possible:

THEOREM 5. *Let p be an odd prime and L/k a cyclic p-extension of CM-fields. Then $\kappa^-_{L/k} = 1$ if and only if one of the following conditions holds*:

(i) $\zeta_p \notin k$;
(ii) $\zeta_p \in k$ *and* $L = k(\zeta_{p^n})$ *for some* $n \geq 2$;
(iii) $\zeta_p \in k$ *and L/k is essentially ramified.*

Moreover, if $\#\kappa^-_{L/k} = p$, *then* $L = k(\sqrt[p]{\beta})$, $\beta\mathcal{O}_k = \mathfrak{b}^p$, *and* $\kappa^-_{L/k} = \langle[\mathfrak{b}]\rangle$.

Proof. Since G is killed by p, so is $\mathrm{H}^{-1}(G, E_L) \simeq {}_NW_L/{}_NW_L \cap E_L^{1-\sigma}$; thus ${}_NW_L = 1$ or ${}_NW_L = \langle\zeta_p\rangle$. We start by showing $\kappa^-_{L/k} = 1$ if one of the conditions (i)–(iii) is satisfied:

(i) In this case, clearly ${}_NW_L = 1$;
(ii) We have $\zeta_p = \zeta_{p^n}^{1-\sigma}$ for a suitable choice of σ, hence ${}_NW_L \subseteq E_L^{1-\sigma}$;
(iii) Assume that $\kappa^-_{L/k} \neq 1$; then it has order p, and there exists an ideal class $c = [\mathfrak{a}] \in \mathrm{Cl}_p^-(k)$ such that $\mathfrak{a}\mathcal{O}_L = \alpha$ and $\alpha^{1-\sigma} = \zeta_p$. This implies $(\alpha^p)^{1-\sigma} = 1$, i.e. $\beta = \alpha^p \in k$, and thus $K = k(\sqrt[p]{\beta})$. But now $\beta\mathcal{O}_k = \mathfrak{a}^p$, and K/k is not essentially ramified.

Now assume that $\kappa^-_{L/k} = 1$; if (i) holds, then we are done, hence we may assume that $\zeta_p \in k$. Since K/k is cyclic, there exists a $\beta \in k$ such that $K = k(\sqrt[p]{\beta})$. If (iii) holds, i.e. if K/k is essentially ramified, we are done; assume therefore that $\beta\mathcal{O}_k = \mathfrak{b}^p$ for some integral ideal $\mathfrak{b}$. Since L/F is normal, we must have $\beta^{1+J} = \xi^p$ for some $\xi \in k^\times$ by Galois theory; thus $(\beta)^{1+J} = (\mathfrak{b}^p)^{1+J} = (\xi)^p$, and we get $\mathfrak{b}^{1+J} = (\xi)$, in other words, $[\mathfrak{b}] \in \mathrm{Cl}^-(k)$. But $\mathfrak{b}\mathcal{O}_L = k(\sqrt[p]{\beta})$ shows that $\mathfrak{b}$ capitulates, and now our assumption $\kappa^-_{L/k} = 1$ implies that $\mathfrak{b}\mathcal{O}_k = (\alpha)$ is principal. Thus $\beta = \alpha^p\varepsilon$ for some unit $\varepsilon \in E_k$. Since $\varepsilon^2 = \zeta\eta$ for some root of unity $\zeta \in W_k$ and a real unit $\eta \in E_{k^+}$, we find

$$L = k(\sqrt[p]{\beta}) = k(\sqrt[p]{\alpha^p\varepsilon}) = k(\sqrt[p]{\varepsilon}) = k(\sqrt[p]{\varepsilon^2}) = k(\sqrt[p]{\zeta\eta}).$$

But now $\beta^{1+J} = \xi^p$ implies that $\eta^2 = (\zeta\eta)^{1+J}$ is also a pth power in $k^\times$, and we finally find $L = k(\sqrt[p]{\zeta})$, i.e. we are in case (ii). The last remark follows from the second half of our proof. ∎

8. Blowing up class groups. In this section we will study the behaviour of ideal class groups under transfer in cyclic extensions. The starting point of our considerations was the following observation: let k be a subfield of $K = \mathbb{Q}(\zeta_n)$, and assume that a prime $p \nmid (K : k)$ divides the class number

$h(k)$ of k; then the transfer of ideal classes $j : \mathrm{Cl}(k) \to \mathrm{Cl}(K)$ is injective, and $p \mid h(K)$.

Take for example $n = 23$ and $k = \mathbb{Q}(\sqrt{-23})$: here $3 \mid h(k)$, $(K : k) = 11$, and hence $3 \mid h(K)$. This simple method does, however, not explain why $3 \mid h(K)$ for $K = \mathbb{Q}(\zeta_{31})$: although $k = \mathbb{Q}(\sqrt{-31})$ has class number 3, the degree $(K : k) = 15$ is divisible by 3. From Theorem 5 we know that $j : \mathrm{Cl}(k) \to \mathrm{Cl}(K)$ is injective in this case also (since $\mathrm{Cl}(k) = \mathrm{Cl}^-(k)$), hence $3 \mid h(K)$. The class number formula, on the other hand, shows that even $3^2 \mid h(K)$. This is explained by the following proposition, which generalizes a result in [21] (Satz 2 and §4):

PROPOSITION 10. *Let K/k be a ramified cyclic extension of prime degree p, put $r = \operatorname{rank} \mathrm{Cl}_p(k)$, and let γ denote the rank of $\kappa_{K/k}$. Then $\#\,\mathrm{Cl}_p(K) \geq p^{r-\gamma}\,\#\,\mathrm{Cl}_p(k)$.*

Proof. Consider the exact sequence

$$1 \to {}_N\mathrm{Cl}_p(K) \to \mathrm{Cl}_p(K) \xrightarrow{N} \mathrm{Cl}_p(k) \to 1. \tag{2}$$

Here the norm map $N : \mathrm{Cl}_p(K) \to \mathrm{Cl}_p(k)$ is onto by class field theory since K/k is ramified, and ${}_N\mathrm{Cl}_p(K)$ is the kernel of this map by definition. Now clearly $\kappa \subseteq {}_p\mathrm{Cl}(k) := \{c \in \mathrm{Cl}(k) : c^p = 1\}$ and ${}_p\mathrm{Cl}(k)^j \subseteq {}_N\mathrm{Cl}_p(K)$; this shows immediately that $\#_N\mathrm{Cl}_p(K) \geq \#_p\mathrm{Cl}(k)^j \geq ({}_p\mathrm{Cl}(k) : \kappa) = p^{r-\gamma}$. ∎

EXAMPLE. Put $k = \mathbb{Q}(\sqrt{229})$, and let K be the sextic subfield of $\mathbb{Q}(\zeta_{229})$. Computations ([16]) show that $h(k) = h(K) = 3$: now Proposition 10 says that the class group of k capitulates in K.

For our next result, we will need some results of Inaba [7] (see Gras [4] for a modern exposition) on Galois modules of cyclic groups. Let $G = \langle\sigma\rangle$ be a finite group of prime order p, and let M be a finite G-module of order p^t for some $t \in \mathbb{N}$. Define the submodules $M_k = \{m \in M : m^{(1-\sigma)^k} = 1\}$ and $M^{(k)} = \{m \in M : m^{p^k} = 1\}$, and let $\nu = 1+\sigma+\sigma^2+\ldots+\sigma^{p-1} = j \circ N$ denote the "algebraic norm" on M. Then

1. $1 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = M$ for a sufficiently big $n \in \mathbb{N}$. Moreover, $M_j = M_{j+1}$ if and only if $M_j = M$;
2. $(M_n : M_{n-1}) \leq \ldots \leq (M_2 : M_1) \leq \#M_1$;
3. If $M^\nu = 1$, then $M^{(n)} = M_{n(p-1)}$, and in particular $\#M_1 \leq (M : M^p) \leq (\#M_1)^{p-1}$; if moreover $M^p \neq 1$, then $(M : M^p) \geq p^{p-2}\#M_1$.

We will also need the existence of polynomials $f, g, h \in \mathbb{Z}[X]$ such that

$$p = (1-\sigma)^{p-1} f(\sigma) + \nu g(\sigma), \tag{3}$$

$$\nu = (1-\sigma)^{p-1} + p h(\sigma). \tag{4}$$

Let K/k be a cyclic extension of prime degree p, and let σ be a generator of the Galois group $G = \mathrm{Gal}(K/k)$. An ideal class c of $\mathrm{Cl}(K)$ is called

ambiguous if it is fixed under the action of G, i.e. if $c^\sigma = c$. The ambiguous ideal classes form a subgroup $\mathrm{Am}(K/k)$ of $\mathrm{Cl}(K)$.

PROPOSITION 11. *If K/k is a cyclic ramified extension of prime degree, then*

$$\#\,\mathrm{Am}(K/k) = ({}_N\mathrm{Cl}(K) : \mathrm{Cl}(K)^{1-\sigma})\#\,\mathrm{Cl}(k);$$

in particular, $\#\,\mathrm{Am}(K/k)$ is divisible by h_k.

P r o o f. Applying the snake lemma to the exact and commutative diagram (note that the surjectivity of the norm map $N : \mathrm{Cl}(K) \to \mathrm{Cl}(k)$ follows from class field theory since K/k is completely ramified)

$$\begin{array}{ccccccccc} 1 & \to & \mathrm{Cl}(K)^{1-\sigma} & \to & \mathrm{Cl}(K)^{1-\sigma} & \to & 1 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & {}_N\mathrm{Cl}(K) & \to & \mathrm{Cl}(K) & \xrightarrow{N} & \mathrm{Cl}(k) & \to & 1 \end{array}$$

and using the fact that the alternating product of the orders of finite groups in an exact sequence is 1, we find

$$({}_N\mathrm{Cl}(K) : \mathrm{Cl}(K)^{1-\sigma}) = (\mathrm{Cl}(K) : \mathrm{Cl}(K)^{1-\sigma})\#\,\mathrm{Cl}(k).$$

Since $(\mathrm{Cl}(K) : \mathrm{Cl}(K)^{1-\sigma}) = \#\,\mathrm{Am}(K/k)$, the claimed equality follows. ∎

In the special case $\gamma = 0$, Theorem 6 below was given (without proof) by Tateyama [31]:

THEOREM 6. *If $(\mathrm{Cl}_p(K) : \mathrm{Cl}_p(k)^j) = p^a$ for some $a \le p - 2 + \gamma$, then $\mathrm{Cl}_p(k)^j = \mathrm{Cl}_p(K)^p$.*

P r o o f. Put $M = \mathrm{Cl}_p(K)$. We claim that $M^{(1-\sigma)^{p-1}} = 1$. In fact, assume that this is false. Then $M_{p-1} \ne M$, hence $p \le (M_p : M_{p-1}) \le \ldots \le (M_2 : M_1)$; this shows $\#M \ge (M : M_{p-1}) \ldots (M_2 : M_1)\#M_1 \ge p^{p-1}\#M_1$. Since $M_1 = \mathrm{Am}_p(K/k)$, we get $\#\,\mathrm{Cl}_p(K) \ge p^{p-1}\#\,\mathrm{Cl}_p(k) = p^{p-1+\gamma}\#\,\mathrm{Cl}_p(k)^j$, where we have used Proposition 11.

Thus $(1-\sigma)^{p-1}$ kills M, and (3) and (4) imply that $M^p = M^\nu$. Since $M^\nu = \mathrm{Cl}_p(k)^j$, the claim follows. ∎

We now define the subgroup ${}_\nu\mathrm{Cl}_p(K)$ by the exact sequence

$$1 \to {}_\nu\mathrm{Cl}_p(K) \to \mathrm{Cl}_p(K) \xrightarrow{\nu} \mathrm{Cl}_p(k)^j \to 1. \tag{5}$$

In other words, ${}_\nu\mathrm{Cl}_p(K)$ is the subgroup of $\mathrm{Cl}_p(K)$ killed by the algebraic norm ν.

PROPOSITION 12. *If $\operatorname{rank}\mathrm{Cl}_p(k)^j \ge \operatorname{rank}\mathrm{Cl}_p(K) - (p-3)$, then ${}_\nu\mathrm{Cl}_p(K)$ is elementary abelian.*

P r o o f. Put $M = {}_\nu\mathrm{Cl}_p(K)$; then $\mathrm{Cl}_p(k)^j \subseteq M_1$, since $\mathrm{Cl}(k)^j$ is clearly killed by $1-\sigma$. If $M^p \ne 1$, then $(M : M^p) \ge p^{p-2}\#M_1$ shows that

$\operatorname{rank}\operatorname{Cl}_p(K) \ge \operatorname{rank} M \ge p-2+\operatorname{rank} M_1 \ge p-2+\operatorname{rank}\operatorname{Cl}(k)^j$, which contradicts our assumption. ∎

THEOREM 7. *If $p \ge 3$ and $\operatorname{rank}\operatorname{Cl}_p(k)^j = \operatorname{rank}\operatorname{Cl}_p(K)$, then $\operatorname{Cl}_p(k)^j = \operatorname{Cl}_p(K)^p$.*

Proof. Since ${}_p\operatorname{Cl}(k)^j \subseteq {}_\nu\operatorname{Cl}_p(K) \subseteq \operatorname{Cl}_p(K)$, our second assumption implies that $\operatorname{rank}{}_\nu\operatorname{Cl}_p(K) = r$. Thus all groups in the exact sequence (5) have the same p-rank, and now our claim follows since ${}_\nu\operatorname{Cl}_p(K)$ is elementary abelian by Proposition 12. ∎

For cyclic extensions $K/\mathbb{Q}$, already Moriya [21] noticed that $\operatorname{Cl}_p(K)$ cannot be cyclic if $\#\operatorname{Cl}_p(K) \ge p^2$. This was generalized by Guerry ([6], Theorem I.9):

COROLLARY 4. *If K/k is a cyclic p-extension ($p \ge 3$), then $\operatorname{Cl}_p(K)$ is cyclic and non-trivial if and only if $\operatorname{Cl}_p(K)/\operatorname{Cl}_p(k)^j \simeq \mathbb{Z}/p\mathbb{Z}$.*

Proof. Assume that $\operatorname{Cl}_p(K)$ is cyclic. If $\operatorname{Cl}_p(k)^j \ne 1$, then $\operatorname{Cl}_p(K)$ and $\operatorname{Cl}_p(k)^j$ have the same rank (i.e. 1), and Theorem 7 proves our claim. Assume therefore that $\operatorname{Cl}_p(k)^j = 1$. Then we have $\operatorname{Cl}_p(K) \simeq \mathbb{Z}/p\mathbb{Z}$ by Inaba's results: put $M = \operatorname{Cl}_p(K)$ and observe that $M^\nu = 1$; if M^p were non-trivial, then $(M : M^p) \ge p^{p-2}\#M_1 \ge p^2$ (since $M \ne 1$ implies $M_1 \ne 1$) shows that M would have rank at least 2, contradicting our assumption. Thus $M^p = 1$, and our claim follows.

For the other direction, assume that $\operatorname{Cl}_p(K)/\operatorname{Cl}_p(k)^j \simeq \mathbb{Z}/p\mathbb{Z}$. Then $a = 1$ in Theorem 6, so $\operatorname{Cl}_p(k)^j = \operatorname{Cl}_p(K)^p$ and $(\operatorname{Cl}_p(K) : \operatorname{Cl}_p(K)^p) = (\operatorname{Cl}_p(K) : \operatorname{Cl}_p(k)^j) = p$, and $\operatorname{Cl}_p(K)$ is cyclic and non-trivial. ∎

REMARK. For odd primes p, all the results in this section hold with $\operatorname{Cl}(K)$, $\operatorname{Cl}_p(K)$ etc. replaced by the corresponding minus class groups $\operatorname{Cl}^-(K)$, $\operatorname{Cl}_p^-(K)$ etc. This follows at once from the following proposition, which shows that there is an exact sequence for the minus part of class groups corresponding to (2).

PROPOSITION 13. *Let K/k be a cyclic extension of CM-fields which is completely ramified. Then the following sequence is exact*:

$$1 \to {}_N\operatorname{Cl}_p^-(K) \to \operatorname{Cl}_p^-(K) \xrightarrow{N} \operatorname{Cl}_p^-(k) \to 1.$$

Proof. We only have to show that the norm $N : \operatorname{Cl}_p^-(K) \to \operatorname{Cl}_p^-(k)$ is surjective. To this end, take a class $c \in \operatorname{Cl}_p^-(k)$, and let J denote complex conjugation; then there is an ideal class $C' \in \operatorname{Cl}_p(K)$ such that $c = NC'$. But $c \in \operatorname{Cl}_p^-(k)$ implies $c = c^{(1-J)/2}$ since J acts as -1, and we get $c = c^{(1-J)/2} = NC$ for $C = C'^{(1-J)/2}$. Moreover, $C \in \operatorname{Cl}_p^-(K)$ since it is killed by $1+J$. ∎

EXAMPLE. Take $k = \mathbb{Q}(\sqrt{-31})$, and let K be the sextic subfield of $\mathbb{Q}(\zeta_{31})$. Then $\mathrm{Cl}^-(k) \simeq \mathbb{Z}/3\mathbb{Z}$, and the first condition of Theorem 5 shows that no class of $\mathrm{Cl}^-(k)$ capitulates in K. By Proposition 10 we have $h^-(K) \equiv 0 \bmod 9$; the tables in [32] actually show that $h^-(K) = 9$, hence Theorem 6 (applied to the minus part) shows that $\mathrm{Cl}^-(K) \simeq \mathbb{Z}/9\mathbb{Z}$.

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, GP/PARI *calculator*.

[2] P. Cornacchia, *Anderson's module for cyclotomic fields of prime conductor*, preprint, 1997.

[3] G. Cornell and L. Washington, *Class numbers of cyclotomic fields*, J. Number Theory 21 (1985), 260–274.

[4] G. Gras, *Sur les l-classes d'idéaux dans les extensions cubiques relatives de degré l*, Ann. Inst. Fourier (Grenoble) 23 (3) (1973), 1–48.

[5] R. Greenberg, *On some questions concerning the Iwasawa invariants*, Ph.D. thesis, Princeton, 1971.

[6] G. Guerry, *Sur la 2-composante du groupe des classes de certaines extensions cycliques de degré* 2^N, J. Number Theory 53 (1995), 159–172.

[7] E. Inaba, *Über die Struktur der l-Klassengruppe zyklischer Zahlkörper vom Primzahlgrad l*, J. Fac. Sci. Univ. Tokyo Sect. I 4 (1940), 61–115.

[8] K. Iwasawa, *A note on the group of units of an algebraic number field*, J. Math. Pures Appl. 35 (1956), 189–192.

[9] J. F. Jaulent, *L'état actuel du problème de la capitulation*, Sém. Théor. Nombres Bordeaux, 1987/88, exp. 17, 33 pp.

[10] S. Jeannin, *Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer*, J. Théor. Nombres Bordeaux 8 (1996), 75–92.

[11] W. Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. 311/312 (1979), 215–254.

[12] Y. Kida, *l-extensions of CM-fields and cyclotomic invariants*, J. Number Theory 12 (1980), 519–528.

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

[14] —, *Unramified quaternion extensions of quadratic number fields*, J. Théor. Nombres Bordeaux 9 (1997), 51–68.

[15] F. van der Linden, *Class number computations in real abelian number fields*, Math. Comp. 39 (1982), 693–707.

[16] S. Mäki, *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Math. 797, Springer, 1980.

[17] J. Martinet, *Tours de corps de classes et estimations de discriminants*, Invent. Math. 44 (1978), 65–73.

[18] N. Matsumura, *On the class field tower of an imaginary quadratic number field*, Mem. Fac. Sci. Kyushu Univ. Ser. A 31 (1977), 165–177.

[19] R. J. Milgram, *Odd index subgroups of units in cyclotomic fields and applications*, in: Lecture Notes in Math. 854, Springer, 1981, 269–298.

[20] T. Morishima, *On the second factor of the class number of the cyclotomic field*, J. Math. Anal. Appl. 15 (1966), 141–153.

[21] M. Moriya, *Über die Klassenzahl eines relativ-zyklischen Zahlkörpers von Primzahlgrad*, Japan. J. Math. 10 (1933), 1–18.
[22] M. Ozaki, *On the p-rank of the ideal class group of the maximal real subfield of a cyclotomic field*, preprint, 1997.
[23] L. Rédei, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. 49 (1932), 338–363.
[24] L. Rédei und H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933), 69–74.
[25] B. Schmithals, *Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm*, Arch. Math. (Basel) 34 (1980), 307–312.
[26] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. 39 (1934), 95–111.
[27] R. Schoof, *Infinite class field towers of quadratic fields*, J. Reine Angew. Math. 372 (1986), 209–220.
[28] —, *Minus class groups of the fields of the l-th roots of unity*, Math. Comp., to appear.
[29] —, *Class numbers of* $\mathbb{Q}(\cos 2\pi/p)$, to appear (cf. [32], pp. 420–423).
[30] P. Stevenhagen, *On the parity of cyclotomic class numbers*, Math. Comp. 63 (1994), 773–784.
[31] K. Tateyama, *On the ideal class groups of some cyclotomic fields*, Proc. Japan Acad. 58 (1980), 333–335.
[32] L. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, 1997.

Fachbereich 9 Mathematik
Universität des Saarlandes
D-66041 Saarbrücken, Germany
E-mail: franz@math.uni-sb.de

Received on 19.8.1997 (3248)