SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

COLIN D. WALTER

The Ambiguous Class Group and the Genus Group of Certain Non-Normal Extensions

Séminaire de théorie des nombres de Grenoble, tome 7 (1978-1979), exp. n° 7, p. 1-26

<http://www.numdam.org/item?id=STNG_1978-1979__7__A7_0>

Séminaire de Théorie des Nombres
4 octobre 1979
Grenoble

THE AMBIGUOUS CLASS GROUP AND THE GENUS GROUP OF CERTAIN NON-NORMAL EXTENSIONS

par

Colin D. WALTER

In an article generalising work of Roquette and Zassenhaus, Connell and Sussman [2] have demonstrated the importance of certain prime ideals in a number field k_o for estimating the ℓ-rank of the class group of an extension k. These ideals have a power prime to ℓ which is principal and they have prime factors in k with ramification index divisible by ℓ. The products of the prime divisors of these ideals in the normal closure K of k/k_o are invariant under $Gal(K/k_o)$. Thus certain roots in k of the ideals in k_o are fixed by the Galois group. This leads to the concept of ambiguous ideals in an extension k/k_o which is not necessarily normal.

Of particular interest is the case when K/k_o is metacyclic. Then k/k_o is almost a cyclic extension and many of the theorems of cyclic fields have analogues which apply. Since the genus number and the ambiguous class number are equal for a cyclic extension it is worth comparing them in k/k_o. In fact, there they are usually different and this can be seen from the class group description of the genus field. A character theoretic description can also be given for the genus group and this is useful for computing the genus number.

Estimates for the genus number and ambiguous class number have been combined for dihedral extensions by several authors, including Barrucand and Cohn [1] for pure cubic fields. This is done here for pure fields of any odd prime degree over the rational field $\mathbb{Q}$. Indeed, applications to pure fields are the motivating force in this work, and much of the inspiration comes from the class rank estimates of Fröhlich [3] which generalise those of Holzer [8].

1. Ambiguous Classes for Frobenius Extensions

Let G be a Frobenius group with normal kernel N and a complement F. Then G is a semi-direct product of N and F for which the distinct conjugates of F intersect pairwise in the identity. Consequently, if n and f are the orders of N and F respectively then the conjugacy classes of $N-1$ under F all have order f. Hence f divides $n-1$ and is coprime to n.

Suppose K/k_o is a normal extension of number fields whose Galois group is G. Let $L = K^N$ and $k = K^F$ be the fixed subfields of the subgroups N and F. There are many similarities between k/k_o and its lifting by L to the normal extension K/L, but the structure of the latter is generally easier to describe. In this study of the extension k/k_o the analogy between it and the classical case of K/L can be drawn by assuming $f = 1$ so that k/k_o becomes normal.

Denote the (classical) class group of a field Ω by H_Ω, its class number by h_Ω, the n-subgroup of H_Ω by C_Ω, and the maximal subgroup with order prime to n by C_Ω'. Thus $H_\Omega = C_\Omega \times C_\Omega'$.
A class of k will be called <u>ambiguous</u> (over k_o) if its image in H_K is fixed by N (which generates all the conjugates of k/k_o), or, equivalently, by G. The subgroups of such classes are written H_k^G, C_k^G, and $C_k'^G$. Likewise an ideal of k is called <u>ambiguous</u> if its extension to K is fixed under N or, equivalently, under G. A class of H_k is called <u>strongly</u> ambiguous if it contains an ambiguous ideal. These terms are just the standard ones when k/k_o is normal,

and they can easily be generalised still further.

1.1 **Theorem** *The group of ambiguous classes for* k/k_o *is the direct product* $H_k^G = C_k^G \times C_k'^G$. *Here* $C_k'^G$ *is the isomorphic image of* C_{k_o}' *in* C_k' *under the natural embedding given by extension of ideals; and under extension of ideals* C_k^G *is isomorphic to* C_K^G, *the group of ambiguous classes in* K/k_o *with* n*-order. Thus*

$$H_k^G \cong C_K^G \times C_{k_o}'.$$

Proof In Theorem 5.1 of [11] it was shown that the natural maps induced by extension of ideals provide an exact sequence

$$1 \to C_{k_o}' \to C_k' \to C_K'^F / C_K'^G \to 1.$$

Hence any class of C_k' which has its image in C_K' fixed by G comes from a class in C_{k_o}', and *vice versa*.

Since n is prime to $[K:k]$ there is a natural embedding $C_k \hookrightarrow C_K$ which restricts to $C_k^G \hookrightarrow C_K^G$. This is an isomorphism because the inverse map is obtained by applying the idempotent $e_F = f^{-1}\sum_{g\in F} g$ and restriction of ideals, *i.e.* a suitable power of the norm.

Thus the basic observation that provides information about the ambiguous class group of k/k_o is this:

1.2 Lemma C_k^G is isomorphic to the direct summand of the ambiguous n-class group C_K^N of K/L given by the projection e_F, viz. C_K^G.

1.3 Lemma If $\mathfrak{a}$ is an ambiguous ideal of k/k_o then the extension of $N_{k/k_o}\mathfrak{a}$ is equal to $\mathfrak{a}^n$.

Proof The extension of $N_{k/k_o}\mathfrak{a}$ to K is just the product of the conjugates of the extension of $\mathfrak{a}$ under N. However, the extension of $\mathfrak{a}$ is fixed under the action of N and so the product of conjugates is just the nth power. The same equality holds on restriction to k.

Let I_Ω be the multiplicative group of non-zero fractional ideals of a field Ω, extended to K wherever necessary; P_Ω the subgroup of principal ideals; I_Ω^Γ the subgroup of ideals which are fixed by a subgroup Γ of G when extended to K; and $I_\Omega^{\Gamma*}$ the subgroup of ideals which lie in a class of K fixed by Γ. With this notation the isomorphic groups C_k^G and C_K^G are the n-subgroups of I_k^{G*} / P_k and I_K^{G*} / P_K respectively. The most accessible parts of these groups are the subgroups $I_k^G P_k/P_k$ and $I_K^G P_K/P_K$ of strongly ambiguous classes, and in many cases they give the whole group (vid. Corollary 1.9).

Let $\mathfrak{p}$ be a prime ideal of k_o with prime divisors $\mathfrak{q}_j$ in k and below the prime $\mathfrak{P}$ of K. Suppose e, e', e_j, and e'_j are the ramification indices for these primes in K/L, L/k_o, k/k_o, and K/k respectively. The equality $e_j e_j' = ee'$ gives $\mathfrak{p}^n = N_{k/k_o}\mathfrak{p} = \prod_j (N_{k/k_o}\mathfrak{q}_j)^{ee'/e_j'}$. Hence any common factor between the e'/e_j' divides both n and f and so equals 1. Thus $\mathfrak{q} = \prod \mathfrak{q}_j^{e'/e_j'}$ has no roots in k. Any divisor of $\mathfrak{p}$ in k which is fixed by G must decompose in K as a power of $\mathfrak{Q} = \prod_{g\in H\backslash G}\mathfrak{P}^g$ where H is the decomposition group of $\mathfrak{P}$ over k_o. Therefore such a divisor is a power of $\mathfrak{q} = \mathfrak{Q}^{e'}$ and the generators above $\mathfrak{p}$ of $I_K{}^G$ and $I_k{}^G$ are $\mathfrak{Q}$ and $\mathfrak{q}$ respectively. Since the extensions of $\mathfrak{p}$ are equal to $\mathfrak{q}^e$ for k and $\mathfrak{Q}^{ee'}$ for K the powers of $\mathfrak{Q}$ and $\mathfrak{q}$ cannot generate ideal classes with n-order in H_K or H_k other than those of the powers of the extensions of $\mathfrak{p}$ unless $e > 1$, <u>i.e.</u> the prime ideal $\mathfrak{p}$ ramifies in K/L. Hence $I_K{}^G$ and $I_k{}^G$ are generated (the former up to an index prime to n) by I_L and I_{k_o} respectively, together with the ideals $\mathfrak{Q}$ and $\mathfrak{q}$ respectively which divide the prime ideals $\mathfrak{p} \in I_{k_o}$ which are ramified in K/L.

Put $e_{\mathfrak{p}}$ for the ramification index in K/L of a prime ideal $\mathfrak{p} \in I_{k_o}$. Then,

1.4 <u>Lemma</u> $[I_k{}^G : I_{k_o}] = \prod_{\mathfrak{p}} e_{\mathfrak{p}}$.

1.5 <u>Remark</u> There are potentially more classes in k to be found from the decomposition of ramified primes: each divisor $\mathfrak{q}_j$ of $\mathfrak{p}$ in k yields some class, but the ideal $\mathfrak{q}$ may only generate certain products of these classes.

From here on suppose N is cyclic, with generator σ. Then F is also cyclic, with generator ϕ say, because it is a subgroup of the cyclic automorphism group of each subgroup of N with prime order. Thus G is metacyclic and, because $f > 1$, n is odd. Write $\tilde{S}$ for the sum in the integral group ring $\mathbb{Z}[G]$ of the elements in a subset S of G. Define $\mathfrak{F} \in \mathbb{Z}[G]$ by $(1-\sigma)\mathfrak{F} = \tilde{F}(1-\sigma)$ and $e_{\mathfrak{F}} = f^{-1}\mathfrak{F}$. Then $\mathfrak{F}$ is determined uniquely up to a multiple of $\tilde{N}$, so that $e_{\mathfrak{F}}$ is really an idempotent of $\mathbb{Z}[G]/\mathbb{Z}[G]\tilde{N}$ which is conjugate to e_F. We have

$$e_F = f^{-1}\tilde{F} \qquad \text{and} \qquad (1-\sigma)e_{\mathfrak{F}} = e_F(1-\sigma).$$

Finally, let E_Ω denote the unit group of a field Ω, $r(\Omega)$ the $\mathbb{Q}$-dimension of $\mathbb{Q} \otimes_{\mathbb{Z}} E_\Omega$ and W the torsion subgroup of E_K. From [11] §3.1, it is known that $W \subset L$ and $W^F \subset k_o$.

1.6 Theorem The number of strongly ambiguous classes for k/k_o is

$$\frac{h_{k_o} \prod_{\mathfrak{p}} e_{\mathfrak{p}}}{|H^1(N, E_K)^{e_{\mathfrak{F}}}|}$$

where the product is over (finite) prime ideals $\mathfrak{p}$ of k_o.

Proof $I_k^G P_k/P_k \cong I_k^G/(I_k^G \cap P_k) \cong (I_k^G/P_{k_o})/(P_k^G/P_{k_o})$. The numerator has order $[I_k^G : I_{k_o}][I_{k_o} : P_{k_o}] = h_{k_o} \prod e_{\mathfrak{p}}$ by 1.4. Since by 1.3 its exponent divides n, the denominator is $P_k^G/P_{k_o} \cong$ $(P_K^N/P_L)^{e_F} \cong (\{\alpha \in K | \alpha^{1-\sigma} \in E_K\}/L^\times E_K)^{e_F} \cong ((K^{1-\sigma} \cap E_K)/E_K^{1-\sigma})^{e_{\mathfrak{F}}} = H^1(N, E_K)^{e_{\mathfrak{F}}}$.

1.7 Corollary The number of strongly ambiguous classes in k/k_o is a multiple of

i) $$\frac{(h_{k_o} \Pi_{\wp} e_{\wp}) [K^{1-\sigma} \cap E_k : E_K^{1-\sigma} \cap k]}{n [E_L : N_{K/L} E_K]}$$

ii) $$\frac{h_{k_o} \Pi_{\wp} e_{\wp}}{n^{r(L)+1} [W : W^G W^n]}$$

iii) $$\frac{h_{k_o} \Pi_{\wp} e_{\wp}}{[k^{n-\tilde{N}} \cap E_K : E_k^{n-\tilde{N}}] [W : W^G W^n]} .$$

The number of strongly ambiguous classes in k/k_o is a divisor of

$$\frac{h_{k_o} \Pi_{\wp} e_{\wp}}{[k^{1-\sigma} \cap W : E_k^{1-\sigma} \cap W]} .$$

Proof Define $\beta_i \in \mathbb{Z}[G]/\mathbb{Z}[G]\tilde{N}$ by $\beta_i = (1-\sigma)^{-i}\tilde{F}(1-\sigma)^i$. Then from [11] §1.7, there is a direct sum decomposition $\mathbb{Z}[G]/\mathbb{Z}[G]\tilde{N} = \bigoplus_{0 \leq i < f} \mathbb{Z}[G]\beta_i$ which yields

$$H^1(N, E_K) = \bigoplus_{0 \leq i < f} H^1(N, E_K)^{\beta_i} .$$

Here β_0 and β_1 can be replaced by e_F and $e_{\mathfrak{F}}$ respectively so that $|H^1(N, E_K)^{e_{\mathfrak{F}}}|$ divides $|H^1(N, E_K)| \, |H^1(N, E_K)^F|^{-1}$. The second factor is just $[K^{1-\sigma} \cap E_k : E_K^{1-\sigma} \cap k]$ whilst the first can be translated using the value $Q(E_K) = n^{-1}$ for the Herbrand quotient given, for example, in [13]. Thus $|H^1(N,E_K)| = n|H^0(N,E_K)| = n[E_L:N_{K/L}E_K]$. This gives (i) from Theorem 1.6.

For (ii) the part of the denominator of 1.6 due to torsion in E_K must be extracted. It is $[k^{1-\sigma}\cap W:E_k^{1-\sigma}\cap W]$. The non-torsion part divides $H^1(N,E_K/W) = n[E_L/W:N_{K/L}E_K/W]$ which itself divides $n^{r(L)+1}$. For $\zeta\in k^{1-\sigma}\cap W$ choose $\alpha\in k$ such that $\zeta=\alpha^{1-\sigma}$. Then $\zeta^n = \zeta^{\tilde N} = \alpha^{(1-\sigma)\tilde N} = 1$ because $W\subset K^N$. Clearly $k_o(\zeta,\alpha)/k_o$ is normal. But G has no normal subgroups other than those containing or contained by N. Thus $\alpha\notin k_o$ implies $L = k_o(\zeta)$. Also $\zeta\in k_o$ implies $\alpha\in k_o$ and hence $\zeta = 1$. So $(k^{1-\sigma}\cap W)/(E_k^{1-\sigma}\cap W)$ is trivial unless possibly when $L\subset k_o(\sqrt[n]{1})$, and then its order divides $[W:W^GW^n]$. In particular, if $k = k_o(\sqrt[n]{\alpha})$ and a prime not dividing n is ramified in k/k_o then α cannot be a unit and $[k^{1-\sigma}\cap W : E_k^{1-\sigma}\cap W] = n$.

For the other parts consider the denominatior of 1.6 again. It comes from $P_k{}^G/P_{k_o} \cong \{\alpha\in k\,|\,\alpha^{1-\sigma}\in E_K\}/k_o{}^{\times}E_k \cong (k^{1-\sigma}\cap E_K)/E_k{}^{1-\sigma}$. This has the factor group $(k^{1-\sigma}\cap E_K)/E_k{}^{1-\sigma}(k^{1-\sigma}\cap W) \cong (k^{1-\sigma}\cap E_K)^{(n-\tilde N)/(1-\sigma)}/E_k{}^{n-\tilde N} \subset (k^{n-\tilde N}\cap E_K)/E_k{}^{n-\tilde N}$ where the isomorphism is given by the class of $\alpha^{1-\sigma}\in k^{1-\sigma}\cap E_K$ mapping to the class of $\alpha^{n-\tilde N}$. This is well-defined: firstly because $\alpha^{1-\sigma}$ determines α up to an element $\beta\in L^{\times}\cap k^{\times} = k_o{}^{\times}$ and $(\alpha\beta)^{n-\tilde N} = \alpha^{n-\tilde N}$ for such β; and secondly because if $\alpha^{1-\sigma} = \zeta\in W$ then $\alpha^{n-\tilde N} = \zeta^{(n-\tilde N)/(1-\sigma)} = \zeta^{n(n-1)/2} = 1$ by the oddness of n. The map is certainly surjective. For the injectivity suppose $\alpha^{1-\sigma}\in k^{1-\sigma}\cap E_K$ maps to $E_k{}^{n-\tilde N}$. Then $(\alpha\varepsilon)^{n-\tilde N} = 1$ for some $\varepsilon\in E_k$. Without loss of generality $\alpha^{n-\tilde N} = 1$ so that $(\alpha^{1-\sigma})^n = (\alpha^n)^{1-\sigma} = \alpha^{\tilde N(1-\sigma)} = 1$

whence $\alpha^{1-\sigma} \in k^{1-\sigma} \cap W$ represents the trivial class. The subgroup initially quotiented out was $(k^{1-\sigma} \cap W)/(E_k^{1-\sigma} \cap W)$ which has order dividing $[W:W^G W^n]$, as was shown above. This completes the proof of (iii) and gives the last part.

Remarks When $n=\ell$ is prime and h_{k_o} is prime to ℓ these estimates give lower bounds for the order of an elementary abelian ℓ-group within the class group of k and hence also a lower bound for the minimal number of generators of its ℓ-Sylow subgroup. Part (iii) and its approximation $h_{k_o} \Pi_{\mathfrak{p}} e_{\mathfrak{p}}/n^{r(k)-r(k_o)+1}$ therefore generalise Frohlich's Theorem 1 in [3] and its proof. This approximation yields the result of Connell and Sussman's Theorem 1 in [2] for k/k_o when the degree is prime; but the analogue for general n may be weaker (vid. 1.5). However, $r(L) + 1 \leqslant r(k) - r(k_o)$ with equality possible only when $f = n-1$. Therefore the estimate in (ii) is at least as good as that from (iii) and the rank interpretation for (ii) generalises Gerth's Proposition 3.4 in [4].

A good knowledge of the unit group of K allows one to obtain still better estimates for the divisibility of h_k:

1.8 Theorem The quotient of ambiguous ideal classes modulo strongly ambiguous classes is isomorphic to

$$((N_{K/L}K^{\times} \cap E_L)/N_{K/L}E_K)^{e_{\mathfrak{z}}} .$$

Proof $(I_k^{G*}/P_k)/(I_k^{G}P_k/P_k) \cong (I_K^{N*})^{e_F}/I_K^{N}P_K$

$\cong (I_K^{N*})^{e_F(1-\sigma)}/(I_K^{N}P_K)^{1-\sigma} = (I_K^{N*})^{(1-\sigma)e_{\mathfrak{F}}}/P_K^{1-\sigma}$

$= \{(\alpha)\,|\,N_{K/L}\alpha \in E_L\}^{e_{\mathfrak{F}}}/P_K^{1-\sigma} \cong \{\alpha \in K\,|\,N_{K/L}\alpha \in E_L\}^{e_{\mathfrak{F}}}/E_K K^{1-\sigma}$

$\cong (N_{K/L}K \cap E_L)^{e_{\mathfrak{F}}}/N_{K/L}E_K$. The first isomorphism is by Lemma 1.2. The subsequent maps are precisely those used by Hasse in [7] Ia §13: multiplication by $1-\sigma$, mapping to a generator of a principal ideal, and applying the norm for K/L. The isomorphisms are proved by him and are straight-forward when Hilbert's Theorem 90 is borne in mind and it is observed that $N_{K/L}$ and $e_{\mathfrak{F}}$ commute.

1.9 Corollary Suppose L/k_o has u unramified infinite primes. Then the quotient of ambiguous classes modulo strongly ambiguous classes has order dividing $n^{uf/2}[W:W^n W^G]$. In particular, when $u=0$ then the quotient is isomorphic to

$$((N_{K/L}K \cap W)/(N_{K/L}E_K \cap W))^{e_{\mathfrak{F}}}.$$

Proof Let C_i be the decomposition group of one infinite prime divisor in K above the infinite prime i of k_o. By hypothesis, C_i has order 2 for all but u valuations i, and without loss of generality $C_i \subset F$ as n is odd. When C_i has order 2 it is generated by $\gamma = \phi^{f/2}$ which inverts elements of N. Write $C_i\mathbb{Z}[G]N$ for the subgroup of $\mathbb{Z}[G]$ fixed on the left by C_i and on the right by N. E_L/W is torsion free and (vid. e.g. [10] §4) is isomorphic to a right submodule of finite index in

$$M = (\oplus_i C_i\mathbb{Z}[G]N)/\mathbb{Z}(\oplus_i \tilde{G}).$$

M is generated by the $\tilde{C}_i g\tilde{N} = g\tilde{C}_i\tilde{N}$ where $g \in F$ and so the effect of $e_{\mathfrak{Z}}$ is determined by the values of $\tilde{C}_i\tilde{N}\mathfrak{Z}$.

Suppose $\phi\sigma\phi^{-1} = \sigma^r$ so that r has order f modulo n and then set

$$\mathfrak{Z} = \sum_{i=0}^{f-1} \left(\sum_{j=0}^{r^i-1} \sigma^j\right)\phi^i - \tilde{N}\sum_{i=0}^{f/2-1} \left(\frac{r^i + r^{i+f/2}}{2n}\right)(\phi^i + \phi^{i+f/2}) .$$

It is immediately verifiable that $(1-\sigma)\mathfrak{Z} = \tilde{F}(1-\sigma)$ and that $\tilde{N}\mathfrak{Z} = \tilde{N}(\gamma-1)\sum_{i=0}^{f/2-1} \frac{1}{2}(r^{i+f/2} - r^i)\phi^i$. Hence $\tilde{C}_i\tilde{N}\mathfrak{Z} = 0$ when C_i has order 2 and $\gamma\tilde{C}_i\tilde{N}\mathfrak{Z} = -\tilde{C}_i\tilde{N}\mathfrak{Z}$ for all i. Thus $M\mathfrak{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ has dimension at most $\frac{1}{2}uf$ over $\mathbb{Q}$ for this choice of $\mathfrak{Z}$. The same is therefore true of $(E_L/W)\mathfrak{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ and shows that $((N_{K/L}K \cap E_L)W/N_{K/L}E_K.W)^{e_{\mathfrak{Z}}}$ has order dividing $n^{uf/2}$.

It remains to consider the subgroup $((N_{K/L}K \cap W)/(N_{K/L}E_K \cap W))^{e_{\mathfrak{Z}}}$ of the group in 1.8 due to torsion in E_K. W^n is contained in the denominator because $\zeta^n = N_{K/L}\zeta$ for $\zeta \in W \subset L$. If $\zeta \in W^G$ then, modulo elements which fix ζ and multiples of n, we have $\mathfrak{Z} \equiv \sum_{i=0}^{f-1} \sum_{j=0}^{r^i-1} \sigma^j\phi^i \equiv \sum_{i=0}^{f-1} r^i = (r^f-1)/(r-1) \equiv 0$. So $(W^G)^{\mathfrak{Z}} \subset W^n$ and there is a natural surjection from $W^G(W \cap N_{K/L}K)/W^nW^G$ to the group under consideration, given by $\zeta/W^nW^G \longrightarrow (\zeta/(N_{K/L}E_K \cap W))^{e_{\mathfrak{Z}}}$. Hence the order of the group divides $[W:W^nW^G]$. The exact sequence

$$1 \longrightarrow (N_{K/L}K \cap W)/(N_{K/L}E_K \cap W) \longrightarrow (N_{K/L}K \cap E_L)/N_{K/L}E_K$$

$$\longrightarrow (N_{K/L}K \cap E_L)W/N_{K/L}E_K.W \longrightarrow 1$$

remains exact when fixed by the idempotent $e_{\mathfrak{F}}$. So the above bounds on the outer two groups of

$$1 \to ((N_{K/L}K \cap W)/(N_{K/L}E_K \cap W))^{e_{\mathfrak{F}}} \to ((N_{K/L}K \cap E_L)/N_{K/L}E_K)^{e_{\mathfrak{F}}}$$

$$\to ((N_{K/L}K \cap E_L)W/N_{K/L}E_K.W)^{e_{\mathfrak{F}}} \to 1$$

place the required bound on the central group and yield the required isomorphism between the first two groups when $u = 0$.

1.10 <u>Corollary</u> <u>Suppose L/k_o has no unramified infinite primes and ζ generates $W \cap N_{K/L}K$ over $W \cap N_{K/L}E_K$. Choose $\alpha \in K$ such that $\zeta = N_{K/L}\alpha$ and an ideal $\mathfrak{a}$ in K for which $(\alpha) = \mathfrak{a}^{1-\sigma}$. Then the class of $N_{K/k}\mathfrak{a}$ generates the ambiguous classes of k/k_o over the strongly ambiguous classes.</u>

<u>Proof</u> Under the maps of 1.8 and 1.9 the image of $N_{K/k}\mathfrak{a}$ is $\zeta^{\mathfrak{F}}$, which generates the group of 1.9.

1.11 <u>Lemma</u> <u>Suppose k/k_o is a pure field extension of a totally real field. Then the quotient of ambiguous by strongly ambiguous classes is isomorphic to</u>

$$(N_{K/L}K \cap W)/(N_{K/L}E_K \cap W).$$

<u>Proof</u> Here L is obtained from k_o by adjoining an nth root of unity ζ, and so L/k_o has no unramified infinite primes. Now ζ generates W/W^n and assuming $\phi\sigma\phi^{-1} = \sigma^r$ gives $\zeta^\phi = \zeta^{r^{-1}}$. So, modulo elements which fix ζ/W^n, $\mathfrak{F} \equiv \sum_{i=0}^{f-1} \sum_{j=0}^{r^i-1} \sigma^j\phi^i \equiv f$. Hence $(W/W^n)^{e_{\mathfrak{F}}} = W/W^n$ and $e_{\mathfrak{F}}$ acts as an automorphism of the group in 1.9. In fact $e_{\mathfrak{F}}$ fixes the group.

2. The Principal Genus of k/k_o.

Let Ω^* denote the Hilbert class field of a field Ω, i.e. its maximal abelian unramified extension, and let Ω^{ab} be its abelian closure. The (relative) genus field of Ω over a subfield Ω_o is defined to be $\Omega^* \cap \Omega\Omega_o^{ab}$; and the associated genus group is the factor group of the class group of Ω corresponding to this extension of Ω. The genus group can also be written as a quotient of the group of ideals in Ω, and then the subgroup factored out is called the principal genus.

As before, suppose K/k_o is a metacyclic Frobenius extension. Then K/L is cyclic of odd degree n and its (relative) principal genus is known to be $P_K I_K^{1-\sigma}$ where σ generates $Gal(K/L)$ (vid. [13]). Hasse's analogue ([7] Ia §13) of Hilbert's Theorem 90 shows that this is precisely the group $P_K \operatorname{Ker} N_{K/L}$ where $\operatorname{Ker} N_{K/L}$ is the kernel of the norm map $I_K \to I_L$. Thus $\mathfrak{a} \in I_K$ is in the principal genus if, and only if, $N_{K/L}\mathfrak{a} = N_{K/L}(\alpha)$ for some $\alpha \in K$. This interpretation also holds for the principal genus of k/k_o by Theorem 2.2 (iii). However, the genus number and the ambiguous class number, which coincide for K/L need not be equal for k/k_o.

The analogue to Hilbert's Theorem 90 for k/k_o is:

2.1 Lemma i) If $\alpha \in k$ and $N_{k/k_o}\alpha = 1$ then $\alpha = N_{K/k}(\beta^{1-\sigma})$ for some $\beta \in K^\times$;

ii) If $\mathfrak{a} \in I_k$ and $N_{k/k_o}\mathfrak{a} = (1)$ then $\mathfrak{a} = N_{K/k}(\mathfrak{b}^{1-\sigma})$ for some $\mathfrak{b} \in I_K$.

<u>Proof</u> Let S be a set of representatives for the conjugacy classes of $N-1$ under F. If $N_{k/k_o}\alpha = 1$ then $\alpha = \beta^{1-\sigma}$ for some $\beta\epsilon K^\times$ by Hilbert's Theorem 90. Here $\beta^{1-\sigma}$ is fixed by F and so $\alpha = \beta^{1-\sigma} = (\beta^{1-\sigma})^{\tilde{N}-\sum_{h\epsilon F}\sum_{g\epsilon S}hgh^{-1}} = (\beta^{1-\sigma})^{-\tilde{S}\tilde{F}} = (\beta^{-\tilde{S}})^{(1-\sigma)\tilde{F}} = N_{K/k}((\beta^{-\tilde{S}})^{1-\sigma})$, as required. The second part is analogous using Hasse's lemma (<u>op.cit.</u>).

2.2 <u>Theorem</u> i) <u>The ambiguous class number of</u> k/k_o <u>is</u>

$$|C_{k_o}'|\,|C_K^F|/|C_K^{F(1-\sigma)}|.$$

ii) <u>The genus group of</u> k/k_o <u>is isomorphic to</u>

$$C_{k_o}' \times C_K^F/C_K^{(1-\sigma)F}.$$

iii) <u>The (relative) principal genus of</u> k/k_o <u>is</u> $P_k I_K^{(1-\sigma)\tilde{F}}$, i.e. <u>the group of ideals</u> $\mathfrak{A} \epsilon I_k$ <u>such that</u> $N_{k/k_o}\mathfrak{A} = N_{k/k_o}(\alpha)$ <u>for some</u> $\alpha\epsilon k$.

A comparison of (i) and (ii) shows that for k/k_o the ambiguous class number will differ from the genus number if $C_K^{F(1-\sigma)}$ and $C_K^{(1-\sigma)F}$ have different orders. This is usually the case for pure fields (<u>vid.</u> Section 3).

<u>Proof</u> The first part is just Theorem 1.1 and the exactness of

$$1 \to C_K^G \to C_K^F \to C_K^{F(1-\sigma)} \to 1.$$

The maximal abelian extension of k_o unramified over k and with degree prime to n is unramified over k_o and so corresponds to the class group C_{k_o}'. The maximal abelian n-extension of k_o unramified over k is the maximal abelian n-extension of k_o unramified over K. It is therefore the maximal abelian n-extension of L in K^* which is fixed under F (<u>i.e.</u> under the action of $Gal(L/k_o)$ suitably extended). The corresponding genus group for this field is $C_K/C_K^{1-e_F}C_K^{1-\sigma}$ because the group for the class field of k is $C_K/C_K^{1-e_F} \cong C_K^F$ and the genus group for K/L is $C_K/C_K^{1-\sigma}$. Part (ii) now follows from the exactness of

$$1 \to (C_K^{1-\sigma})^F \to C_K^F \to C_K/C_K^{1-e_F}C_K^{1-\sigma} \to 1.$$

The genus group itself is therefore $H_k/C_k'^{1-e_N}C_K^{(1-\sigma)\tilde{F}}$ where $e_N = n^{-1}\tilde{N}$. Hence the principal genus is the group of ideals with class belonging to $C_k'^{1-e_N}C_K^{(1-\sigma)\tilde{F}}$. From 2.1(ii) this group is included in $P_kI_K^{(1-\sigma)\tilde{F}}$. Conversely, if $\mathfrak{a} \in I_K$ and $\mathfrak{a}^{(1-\sigma)\tilde{F}}$ is in a class of C_k' then $\mathfrak{a}^{(1-\sigma)\tilde{F}(n-\tilde{N})} = \mathfrak{a}^{(1-\sigma)\tilde{F}n}$ is in a class of $C_k'^{1-e_N}$. So $\mathfrak{a}^{(1-\sigma)\tilde{F}}$ is in a class of $C_k'^{1-e_N}$, and the principal genus is indeed $P_kI_K^{(1-\sigma)\tilde{F}}$. The equivalence of the other formulation in (iii) is clear using 2.1(ii).

2.3 <u>Corollary</u> <u>The genus group of</u> k/k_o <u>is isomorphic to</u> $N_{k/k_o}I_k/N_{k/k_o}P_k$.

<u>Proof</u> Apply $\tilde{N}$ to $I_k/P_kI_K^{(1-\sigma)\tilde{F}}$, which is the genus group, and use the alternative definition of the principal genus in 2.2(iii) to show this is a monomorphism.

Now if $a \in k_o^\times$ and $a = N_{K/L}\alpha$ then $a = N_{k/k_o}(a/N_{K/k}\alpha^{(n-1)/f})$.
Hence:

2.4 Lemma *$a \in k_o$ is a norm in k/k_o if, and only if, it is a norm in K/L.*

For each prime ideal $\mathfrak{p}_i$ $(1 \leq i \leq t)$ of k_o which is ramified in K/L let $\mathfrak{P}_i$ be a prime of L above $\mathfrak{p}_i$ and for $a \in k_o^\times$ let $\chi_i(a) = \left(\frac{a, K/L}{\mathfrak{P}_i}\right)$ be the norm residue symbol. This yields a map $\chi : k_o^\times \to N^t$ defined by $\chi(a) = (\chi_1(a), \chi_2(a), \ldots, \chi_t(a))$.

2.5 Lemma *$a \in k_o^\times$ is a norm in k/k_o if, and only if, $a \in \ker\chi$.*

Proof a is a norm in k/k_o <=> a is a norm in K/L (by 2.4) <=> a is a local norm for every completion of K/L (since K/L is cyclic) <=> a is a local norm for each prime ideal of L ramified in K (since the oddness of n ensures that no infinite valuation is ramified) <=> $\left(\frac{a, K/L}{\mathfrak{P}}\right) = 1$ for each conjugate $\mathfrak{P}$ of each prime ideal $\mathfrak{P}_i$ <=> $\left(\frac{a, K/L}{\mathfrak{P}_i}\right) = 1$ for $1 \leq i \leq t$ (since $\left(\frac{a, K/L}{\mathfrak{P}_i^\tau}\right) = \tau^{-1}\left(\frac{a, K/L}{\mathfrak{P}_i}\right)\tau$ for $\tau \in \mathrm{Gal}(L/k_o)$) $\Leftrightarrow$ $\chi(a) = 1$.

Suppose ${}_N I_k$ is the group of ideals in k which have principal norms in k_o. If $\mathfrak{a} \in {}_N I_k$ and $N_{k/k_o}\mathfrak{a} = (a)$ for $a \in k_o$ then a homomorphism $\mathcal{X} : {}_N I_k \to \chi(k_o)/\chi(E_{k_o})$ can be defined by $\mathcal{X}(\mathfrak{a}) = \chi(a) \bmod \chi(E_{k_o})$.

2.6 **Theorem** (cf. [5] & [6]) $\ker\chi$ *is the principal genus of* k/k_o.

Proof Assume $\mathfrak{a} \in {}_N I_k$ satisfies $N_{k/k_o}\mathfrak{a} = (a)$. Then by Theorem 2.2(iii) $\mathfrak{a}$ is in the principal genus if, and only if, $a\varepsilon$ is a norm in k/k_o for some unit ε of k_o, *i.e.* if, and only if, $a\varepsilon \in \ker\chi$.

When the class number of k_o is prime to n the map $\mathcal{X}$ can be extended to the whole of I_k. Choose $h \in \mathbb{Z}$ such that $hh_{k_o} \equiv 1 \bmod n$. For $\mathfrak{a} \in I_k$ with $N_{k/k_o}\mathfrak{a}^{h_{k_o}} = (b)$ we must have $\mathcal{X}(\mathfrak{a})^n = 1$ and therefore $\mathcal{X}(\mathfrak{a}) = \mathcal{X}(\mathfrak{a}^{hh_{k_o}}) = \chi(b^h) \bmod \chi(E_{k_o})$. This is consistent with $\mathcal{X}$ on ${}_N I_k$ as defined above. Clearly for this extended map $\ker\mathcal{X}$ is the group of ideals whose h_{k_o} th power is in the principal genus. Hence:

2.7 **Theorem** *When* h_{k_o} *is prime to* n *the* n-*subgroup of the genus group of* k/k_o *is isomorphic to* $\mathcal{X}(I_k)$.

2.8 **Corollary** *When* h_{k_o} *is prime to* n *the genus number of* k/k_o *divides*

$$\frac{h_{k_o} n^t}{[E_{k_o} : E_{k_o} \cap N_{k/k_o} k]} .$$

Proof $\mathcal{X}(I_k)$ is a subgroup of $\chi(k_o^\times)/\chi(E_{k_o})$ and this is a subgroup of $N^t/\chi(E_{k_o})$, which has order $n^t/[E_{k_o} : N_{k/k_o} k \cap E_{k_o}]$. By the theorem this bounds the n-component of the genus number, and the factor prime to n is given precisely by Theorem 2.2(ii).

<u>Remark</u> Putting $f = 1$ and using the product formula for norm residue symbols to replace t by $t-1$ in 2.8 provides the familiar formula for the genus number of K/L.

3. Pure Fields of Prime Degree over $\mathbb{Q}$

Let ℓ be an odd rational prime, ζ a primitive ℓth root of unity, and m a positive ℓth power free rational integer. For this section let $k_o = \mathbb{Q}$, $k = \mathbb{Q}(\sqrt[\ell]{m})$, $L = \mathbb{Q}(\zeta)$, and $K = \mathbb{Q}(\sqrt[\ell]{m}, \zeta)$. These fields satisfy the hypotheses of the earlier sections. So the strongly ambiguous classes are generated by the primes of k which are totally ramified over $\mathbb{Q}$. From Wegner [12] these are the prime ideals dividing (m) and, if $m^{\ell-1} \not\equiv 1 \bmod \ell^2$, also the prime ideal above (ℓ). Hence:

3.1 Theorem *Let $\mathfrak{a}$ be an ambiguous ideal of $k = \mathbb{Q}(\sqrt[\ell]{m})$. Then $\mathfrak{a}^\ell = (a)$ for $a \in \mathbb{Q}$ defined by $N_{k/\mathbb{Q}}\mathfrak{a} = (a)$. Here a is a product of ℓth powers, primes dividing m, and, if $m^{\ell-1} \not\equiv 1 \bmod \ell^2$, also the prime ℓ. In the case that $\mathfrak{a}$ is principal, a is a norm.*

3.2 Theorem *For a rational prime p and $a \in \mathbb{Q}^\times$ let $\nu_p(a) \in \mathbb{Z}$ denote the multiplicity of p as a factor of a. Then a is a norm in $k/\mathbb{Q}$ if, and only if,*

$$(m^{\nu_p(a)} a^{-\nu_p(m)})^{(p-1)/\ell} \equiv 1 \bmod p$$

for all primes p dividing m with $p \equiv 1 \bmod \ell$.

Proof By Lemma 2.5 a is a norm in $k/\mathbb{Q}$ if, and only if, $\chi_i(a) = \left(\frac{a, K/L}{\mathfrak{P}_i}\right) = 1$ for $1 \leq i \leq t$. Since there is only one prime ideal in L above (ℓ) the product formula for norm residue symbols permits this prime to be ignored if it occurs. The remaining ramified primes are the $p \neq \ell$ which divide m. Using the properties of Hasse's norm residue and power residue symbols (vid. [7] II §11) for the prime $\mathfrak{P}$ in L above $(p) \neq (\ell)$ one obtains $\left(\frac{a,K/L}{\mathfrak{P}}\right) = \left(\frac{a,m}{\mathfrak{P}}\right) = \left(\frac{p,a^{-\nu_p(m)} m^{\nu_p(a)}}{\mathfrak{P}}\right) = \left(\frac{a^{\nu_p(m)} m^{-\nu_p(a)}}{\mathfrak{P}}\right)$. Let $n(p) = (p^{f(p)}-1)/\ell$ where $f(p)$ is the order of p modulo ℓ. Then $\ell n(p) = N_{L/\mathbb{Q}}\mathfrak{P}-1$. So $\left(\frac{x}{\mathfrak{P}}\right) = 1 \iff x^{n(p)} \equiv 1 \bmod \mathfrak{P} \iff x^{n(p)} \equiv 1 \bmod (p)$ for $x \in \mathbb{Q}$. Thus $\left(\frac{a,K/L}{\mathfrak{P}}\right) = 1 \iff (m^{\nu_p(a)} a^{-\nu_p(m)})^{n(p)} \equiv 1 \bmod p$. This congruence is automatically satisfied when $n(p) \equiv 0 \bmod p-1$, and therefore when ℓ does not divide $p-1$. Otherwise $p \equiv 1 \bmod \ell$, which gives $n(p) = (p-1)/\ell$. The theorem now follows.

3.3 <u>Corollary</u> <u>If</u> $\mathfrak{a}$ <u>is an ambiguous ideal of</u> k <u>with</u> $\mathfrak{a}^{\ell} = (a)$ <u>and</u> a <u>does not satisfy all the congruences of Theorem 3.2 then</u> $\mathfrak{a}$ <u>is not principal</u>.

<u>Proof</u> Combine Theorems 3.1 and 3.2.

Let $\{p_i | 1 \leq i \leq t\}$ be the set of ramified primes as described above, and let $\{p_i | 1 \leq i \leq s\}$ be the subset of $p \equiv 1 \bmod \ell$. Define $\chi_i'(a) = (m^{\nu_p(a)} a^{-\nu_p(m)})^{(p-1)/\ell} \bmod p$ for $p = p_i$ and $1 \leq i \leq s$. Then $\chi'(a) = (\chi_1'(a), \chi_2'(a), \ldots, \chi_s'(a))$ provides a homomorphism in effect from $\mathbb{Q}^{\times}$ to $\mathbb{F}_{\ell}^{s}$ where $\mathbb{F}_{\ell}$ is the finite field of ℓ elements. By 3.2 the kernel of χ' is the subgroup of $a \in \mathbb{Q}^{\times}$ which are norms in $k/\mathbb{Q}$. Composing this with the map $\nu : I_k \to \mathbb{Q}^{\times}$ given by

$\mathfrak{a} \mapsto |a|$ for $N_{k/\mathbb{Q}}\mathfrak{a} = (a)$ yields a homomorphism $\mathcal{N}' : I_k \to \mathbb{F}_\ell^{\ s}$. As in §2 the kernel of $\mathcal{N}'$ is the group of ideals whose norms are norms of principal ideals. Thus, as in 2.6 and 2.7,

3.4 Theorem $\ker \mathcal{N}'$ is the principal genus of $k/\mathbb{Q}$ and $|\mathcal{N}'(I_k)|$ is the genus number.

3.5 Theorem i) The genus number of $k/\mathbb{Q}$ is ℓ^s, i.e. $\mathcal{N}'$ is surjective;

ii) the order of $\mathcal{N}'(I_k^{\ N})$ is that of the quotient of strongly ambiguous classes by the subgroup of classes representing ideals of the principal genus;

iii) every ambiguous class is strongly ambiguous, if and only if, $\zeta \in N_{K/L}E_K$ or $\zeta \notin N_{K/L}K$.

Remark ([9] Lemma 4) $\zeta \in N_{K/L}K$ if, and only if, $p_i^{\ell-1} \equiv 1 \bmod \ell^2$ for $1 \leq i \leq t$ with $p_i \neq \ell$. Thus for most m every ambiguous class is strongly ambiguous.

Proof Fröhlich has already proved (i) in [3]. Alternatively, (c.f. [1], Theorem 4.2), let q be a rational prime. Fixing the value of $\chi_i'(q)$ only forces q to belong to certain arithmetic progressions modulo p_i. Hence $\chi' : \mathbb{Q}^\times \to \mathbb{F}_\ell^{\ s}$ is surjective even when restricted to primes $q \equiv 1 \bmod \ell$. But such primes have prime factors $\mathfrak{q}_1$ and $\mathfrak{q}_{\ell-1}$ of degree 1 and $\ell-1$ respectively in k. So $\nu(\mathfrak{q}_1) = q$ and

$\mathcal{N}' = \chi'_0\nu$ is surjective. Note that the ideals $\mathfrak{q}_1$ generate the ℓ^s cosets of the principal genus in I_k, and give rise to an elementary abelian factor group of the class group of k.

The second part comes from Theorem 3.4 and the last part from Lemma 1.11.

3.6 Theorem (c.f. Fröhlich [3] Theorem 3). Let $\ell^{s'}$ be the order of $\mathcal{N}'(I_k^N)$, and let $\ell^{t'}$ be the number of strongly ambiguous classes. Then $t' \geq \max(s', t-(\ell+1)/2)$ and the ℓ-class number of $k = \mathbb{Q}(\sqrt[\ell]{m})$ is divisible by

$$\ell^{s+t'-s'}.$$

Proof By Theorem 3.5(i) the genus group provides ℓ^s cosets of the principal genus and by (ii) of the same theorem the ambiguous ideals provide $\ell^{t'-s'}$ classes in the principal genus. The lower bound on t' is just Corollary 1.7(ii) with Theorem 3.5(ii).

Remark s, t, and s' can be calculated very easily from m and the definition of $\mathcal{N}'$ and so the given lower bound for t' immediately yields a divisor of the ℓ-class number.

References

1 P. Barrucand & H. Cohn. "A Rational Genus, Class Number Divisibility, and Unit Theory for Pure Cubic Fields", J. Number Theory, 2 (1970), 7-21, 3 (1971), 226-239.

2 I. Connell & D. Sussman. "The p-dimension of class groups of number fields", J. London Math. Soc., (2) 2 (1970), 525-529.

3 A. Fröhlich. "On the ℓ-class group of the field $P(\sqrt[\ell]{m})$", J. London Math. Soc., 37 (1962), 189-192.

4 F. Gerth. "On ℓ-class groups of certain number fields", Mathematika, 23 (1976), 116-123.

5 R. Gold. "Genera in Normal Extensions", Pacific J. Math., 63 (1976), 397-400.

6 F. Halter-Koch. "Ein Satz über Geschlechter relativ-zyklischer Zahlkörper von Primzahlgrad und seine Anwendung auf biquadratisch-bizyklische Körper", J. Number Theory, 4 (1972), 144-156.

7 H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, (Physicia-Verlag, Würzburg/Wien, 1970).

8 L. Holzer. "Zur Klassenzahl in reinen Zahlkörpern von ungeraden Primzahlgrade", Acta Math., 83 (1950), 327-348.

9 C. Parry & C. Walter. "The class number of pure fields of prime degree", Mathematika, 23 (1976), 220-226, 24 (1977), 122.

10 C. Walter. "Brauer's class number relation", Acta Arith., 35 (1979), 33-40.

11 C. Walter. "A class number relation in Frobenius extensions of number fields", Mathematatika, 24 (1977), 216-225.

12 U. Wegner. "Zur Theorie der auflösbaren Gleichungen von Primzahlgrad", J.f. reine u. angew. Math., 168 (1932), 176-190.

13 H. Yokoi. "On the class number of a relatively cyclic number field", Nagoya Math. J., 29 (1967), 31-44.

Department of Mathematics,
University College,
Belfield,
Dublin 4, Ireland.

12A35, 12A50: Algebraic Number Theory: global fields: metabelian extensions; class number.