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

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_0 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 all their prime factors in k have ramification index divisible by l. The products of the prime divisors of these ideals in the normal closure K of k/k_0 are invariant under $\mathrm{Gal}(K/k_0)$. Thus certain roots in k of the ideals in k_0 are in some sense fixed by the Galois group. This leads to the concept of ambiguous ideals in an extension k/k_0 which is not necessarily normal.

Of particular interest is the case when K/k_0 is metacyclic. Then k/k_0 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_0. 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 [**4**] which generalise those of Holzer [**9**].

§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_0 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_0 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_0 the analogy between it and the classical case of K/L can be drawn by assuming $f = 1$ so that k/k_0 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 *ambiguous* (over k_0) if its image in H_K is fixed by N (which generates all the conjugates of k/k_0), or, equivalently, by G. The subgroups of such classes are written H_k^G, C_k^G, and C'^G_k. Likewise an ideal of k is called *ambiguous* if its extension to K is fixed under N or, equivalently, under G. A class of H_k is called *strongly* ambiguous if it contains an ambiguous ideal. These terms are just the standard ones when k/k_0 is normal, and they can easily be generalised still further.

1.1 THEOREM. *The group of ambiguous classes for k/k_0 is the direct product* $H_k^G = C_k^G \times C'^G_k$. *Here* C'^G_k *is the isomorphic image of* C'_{k_0} *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_0 with n-order. Thus*

$$H_k^G \cong C_K^G \times C'_{k_0} .$$

Proof. In Theorem 5.1 of [**12**] it was shown that the natural maps induced by extension of ideals provide an exact sequence

$$1 \to C'_{k_0} \to C'_k \to C'^F_K / C'^G_K \to 1 .$$

Hence any class of C'_k which has its image in C'_K fixed by G comes from a class in C'_{k_0}, and *vice versa*.

Since n is prime to $[K : k]$ there is a natural embedding $C_k \rightarrowtail C_K$ which restricts to $C_k^G \rightarrowtail C_K^G$. 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_0 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_0 then the extension of $N_{k/k_0}\,\mathfrak{a}$ is equal to* $\mathfrak{a}^n$.

Proof. The extension of $N_{k/k_0}\,\mathfrak{a}$ 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 (*see* Corollary 1.9).

Let $\mathfrak{p}$ be a prime ideal of k_0 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_0, k/k_0, and K/k respectively. The equality $e_j e'_j = ee'$ gives

$$\mathfrak{p}^n = N_{k/k_0}\,\mathfrak{p} = \prod_j (N_{k/k_0}\,\mathfrak{p}_j)^{ee'/e'_j}$$

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_0. 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 $e > 1$, *i.e.* 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_0} respectively, together with the ideals $\mathfrak{Q}$ and $\mathfrak{q}$ respectively which divide the prime ideals $\mathfrak{p} \in I_{k_0}$ which are ramified in K/L.

Put $e_\mathfrak{p}$ for the ramification index in K/L of a prime ideal $\mathfrak{p} \in I_{k_0}$. Then,

1.4 LEMMA. $[\, I_k^G : I_{k_0}] = \prod_\mathfrak{p} e_\mathfrak{p}$.

1.5 *Remark*. 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 ring $\mathbb{Z}[G]$ of the elements in a subset S of G. Define $\mathscr{F} \in \mathbb{Z}[G]$ by $(1-\sigma)\mathscr{F} = \tilde{F}(1-\sigma)$ and $e_\mathscr{F} = f^{-1}\mathscr{F}$. Then $\mathscr{F}$ is determined uniquely up to a multiple of $\tilde{N}$, so that $e_\mathscr{F}$ is really an idempotent of $\mathbb{Q}[G]/\mathbb{Q}[G]\tilde{N}$ which is conjugate to e_F. We have

$$e_F = f^{-1}\tilde{F} \qquad \textit{and} \qquad (1-\sigma)e_\mathscr{F} = e_F(1-\sigma)\,.$$

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 [**12**] §3.1, it is known that $W \subset L$ and $W^F \subset k_0$.

1.6 THEOREM. *The number of strongly ambiguous classes for* k/k_0 *is*

$$\frac{h_{k_0}\prod_\mathfrak{p} e_\mathfrak{p}}{\left|H^1(N,E_K)^{e_\mathscr{F}}\right|}\,,$$

where the product is over (*finite*) *prime ideals* $\mathfrak{p}$ *of* k_0.

Proof. $I_k^G P_k / P_k \cong I_k^G/(I_k^G \cap P_k) \cong (I_k^G / P_{k_0})/(P_k^G / P_{k_0})$. The numerator has order $[I_k^G : I_{k_0}][I_{k_0} : P_{k_0}] = h_{k_0}\prod e_\mathfrak{p}$ by 1.4. Since by 1.3 its exponent divides n, the denominator is

$$P_k^G/P_{k_0} \cong (P_K^N/P_L)^{e_F} \cong (\{\alpha \in K \mid \alpha^{1-\sigma} \in E_K\}/L^\times E_K)^{e_F}$$
$$\cong ((K^{1-\sigma} \cap E_K)/E_K^{1-\sigma})^{e_{\mathscr{F}}} = H^1(N,E_K)^e\,.$$

1.7 COROLLARY. *The number of strongly ambiguous classes in k/k_0 is a multiple of*

$$(i)\quad \frac{(h_{k_0}\prod_{\mathfrak{p}} e_{\mathfrak{p}})[K^{1-\sigma} \cap E_k : E_K^{1-\sigma} \cap k]}{n[E_L : N_{K/L}E_K]}$$

and

$$(ii)\quad \frac{h_{k_0}\prod_{\mathfrak{p}} e_{\mathfrak{p}}}{[k^{n-\tilde{N}} \cap E_K : E_k^{n-\tilde{N}}][W : W^G W^n]}\,.$$

The number of strongly ambiguous classes in k/k_0 is a divisor of

$$\frac{h_{k_0}\prod_{\mathfrak{p}} e_{\mathfrak{p}}}{[k^{1-\sigma} \cap W : E_k^{1-\sigma} \cap W]}$$

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 [**12**] §1.7, there is a direct sum decomposition

$$\mathbb{Z}[G]/\mathbb{Z}[G]\tilde{N} \quad = \quad \bigoplus_{0\le i<f}\mathbb{Z}[G]\beta_i$$

which yields

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

Here β_0 and β_i can be replaced by e_F and $e_{\mathscr{F}}$ respectively so that $|H^1(N,E_K)^{e_{\mathscr{F}}}|$ 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 Herband quotient given, for example, in [**14**]. 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.

Bounds can be obtained for the denominator of the last part. 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 $k_0(\zeta,\alpha)/k_0$ is normal. But G has no normal subgroups other than those containing or contained by N. Thus $\alpha \notin k_0$ implies $L = k_0(\zeta)$. Also $\zeta \in K_0$ implies $\alpha \in k_0$ and hence $\zeta = 1$. So $(k^{1-\sigma} \cap W)/(E_k^{1-\sigma} \cap W)$ is trivial unless possibly when $L \subset k_0(\sqrt[n]{1})$, and then its order divides $[W : W^G W^n]$. In particular, if $k = k_0(\sqrt[n]{\alpha})$ and a prime not dividing n is ramified in k/k_0 then α cannot be a unit and $[k^{1-\sigma} \cap W : E_k^{1-\sigma} \cap W] = n$.

For the rest consider the denominator of 1.6 again. It comes from

$$P_k^G/P_{k_0} \cong \{\alpha \in k \mid \alpha^{1-\sigma} \in E_K\}/k_0^\times E_k \cong (k^{1-\sigma} \cap E_K)/E_k^{1-\sigma}\,.$$

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

$\beta \in L^\times \cap k^\times = k_0^\times$ 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 (ii) and gives the last part.

Remarks. When $n = l$ is prime and h_{k_0} 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 (ii) and its approximation $h_{k_0}\prod_{\mathfrak{p}} e_{\mathfrak{p}}/n^{r(k)-r(k_0)+1}$ therefore generalise Fröhlich's Theorem 1 in [**4**] and its proof. This approximation yields the result of Connell and Sussman's Theorem 1 in [**2**] for k/k_0 when the degree is prime; but the analogue for general n may be weaker (see 1.5). However, $r(L)+1 \leq r(k)-r(k_0)$ with equality possible only when $f = n-1$. Therefore the estimate in (i) is usually as good as that from (ii) and the rank interpretation for (i) generalises Gerth's Proposition 3.4 in [**5**].

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*

$$((N_{K/L}K \cap E_L)/N_{K/L}E_K)^e$$

Proof.
$$\begin{aligned}(I_k^{G*}/P_k)/(I_k^G P_k/P_k) &\cong (I_K^{N*})^{e_F}/(I_K^N P_K)\\ &\cong (I_K^{N*})^{e_F(1-\sigma)}/(I_K^N P_K)^{1-\sigma} = (I_K^{N*})^{(1-\sigma)e_{\mathscr{F}}}/P_K^{1-\sigma}\\ &= \{(\alpha) \mid N_{K/L}\alpha \in E_L\}^e/P_K^{1-\sigma}\\ &\cong \{\alpha \in K \mid N_{K/L}\alpha \in E_L\}^e/E_K K^{1-\sigma}\\ &\cong (N_{K/L}K \cap E_L)^e/N_{K/L}E_K.\end{aligned}$$

The first isomorphism is by Lemma 1.2. The subsequent maps are precisely those used by Hasse in [**8**] 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 straightforward when Hilbert's Theorem 90 is borne in mind and it is observed that $N_{K/L}$ and $e_{\mathscr{F}}$ commute.

1.9 COROLLARY. *Suppose L/k_0 has u unramified infinite primes. Then the quotient of ambiguous classes modulo strongly ambiguous classes has order dividing $n^{uf/2}[W : W^n W^G]$ for even f. In particular, when $u = 0$ the quotient is isomorphic to*

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

Proof. Let C_i be the decomposition group of one infinite prime divisor in K above the infinite prime i of k_0. 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 (*see e.g.* [**11**] §4) is isomorphic to a right submodule of finite index in

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

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 $e_{\mathscr{F}}$ is determined by the values of $\tilde{C}_i\tilde{N}\mathscr{F}$.

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

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

It is immediately verifiable that $(1-\sigma)\mathscr{F} = \tilde{F}(1-\sigma)$ and that

$$\tilde{N}\mathscr{F} = \tilde{N}(\gamma-1)\sum_{i=0}^{f/2-1}\tfrac{1}{2}(r^{i+f/2}-r^i)\phi^i.$$

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

It remains to consider the subgroup $((N_{K/L}K\cap W)/(N_{K/L}E_K\cap W))^{e_{\mathscr{F}}}$ 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

$$\mathscr{F} \equiv \sum_{i=0}^{f-1}\sum_{j=0}^{r^i-1}\sigma^j\phi^i \equiv \sum_{i=0}^{f-1}r^i = (r^f-1)/(r-1)\equiv 0.$$

So $(W^G)^{\mathscr{F}}\subset W^n$ and there is a natural surjection from $(W\cap N_{K/L}K)W^G / W^nW^G$ to the group under consideration, given by $\zeta/W^nW^G \mapsto (\zeta/(N_{K/L}E_K\cap W))^{e_{\mathscr{F}}}$. Hence the order of the group divides $[W : W^nW^G]$. The exact sequence

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

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

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

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

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

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

1.10. COROLLARY. *Suppose L/k_0 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_0 over the strongly ambiguous classes.*

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

1.11 LEMMA. *Suppose k/k_0 is a pure field extension of a totally real field. Then the quotient of ambiguous by strongly ambiguous classes is isomorphic to*

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

Proof. Here k is obtained from k_0 by adjoining a root of an element in k_0. Therefore L is obtained from k_0 by adjoining an nth root of unity ζ and so L/k_0 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,

$$\mathscr{F} \equiv \sum_{i=0}^{f-1}\sum_{j=0}^{r^i-1} \sigma^j\phi^i \equiv f.$$

Hence $(W/W^n)^{e_{\mathscr{F}}} = W/W^n$ and $e_{\mathscr{F}}$ acts as an automorphism of the group in 1.9. In fact $e_{\mathscr{F}}$ fixes the group.

§2. *The Principal Genus of k/k_0*. A definition of genus for a general finite extension of the rationals was first given in [**3**] by Fröhlich. Here the notion of relative genus over a base field is required and it is defined as follows (*see* [**14**]). 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_0 is defined to be $\Omega^* \cap \Omega\Omega_0{}^{ab}$; 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_0 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) (*see* [**14**]). Hasse's analogue ([**8**] Ia §13) of Hilbert's Theorem 90 shows that this is precisely the group P_K Ker $N_{K/L}$ where 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_0 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_0 .

The analogue of Hilbert's Theorem 90 for k/k_0 is:

2.1 LEMMA. (i) *If $\alpha \in k$ and $N_{k/k_0}\alpha = 1$ then $\alpha = N_{K/k}(\beta^{1-\sigma})$ for some $\beta \in K^{\times}$* ;

(ii) *If $\mathfrak{a} \in I_k$ and $N_{k/k_0}\mathfrak{a} = (1)$ then $\mathfrak{a} = N_{K/k}(\mathfrak{b}^{1-\sigma})$ for some $\mathfrak{b} \in I_K$.*

Proof. Let S be a set of representatives for the conjugacy classes of N–1 under F. If $N_{k/k_0}\alpha = 1$ then $\alpha = \beta^{1-\sigma}$ for some $\beta \in K^{\times}$ by Hilbert's Theorem 90. Here $\beta^{1-\sigma}$ is fixed by F and so

$$\alpha = \beta^{1-\sigma} = (\beta^{1-\sigma})^{\tilde{N} - \sum_{h\in F}\sum_{g\in S} hgh^{-1}} = (\beta^{1-\sigma})^{-\tilde{S}\tilde{F}} = (\beta^{-\tilde{S}})^{(1-\sigma)\tilde{F}} = N_{K/k}((\beta^{-\tilde{S}})^{1-\sigma}),$$

as required. The second part is analogous using Hasse's lemma (*op. cit.*).

2.2 THEOREM. (i) *The ambiguous class number of k/k_0 is*

$$|\, C'_{k_0} \,||\, C_K^F \,| \,/\, |\, C_K^{F(1-\sigma)} \,| \ .$$

(ii) *The genus group of k/k_0 is isomorphic to*

$$C'_{k_0} \times C_K^F / C_K^{(1-\sigma)F} \quad .$$

(iii) *The* (*relative*) *principal genus of k/k_0 is $P_k I_K^{(1-\sigma)\tilde{F}}$, i.e., the group of ideals $\mathfrak{a} \in I_k$ such that $N_{k/k_0}\mathfrak{a} = N_{k/k_0}(\alpha)$ for some $\alpha \in k$.*

A comparison of (i) and (ii) shows that for k/k_0 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 (*see* Section 3).

Proof. 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_0 , unramified over k, and with degree prime to n, is unramified over k_0, and so corresponds to the class group C'_{k_0}. The maximal abelian n-extension of k_0 unramified over k is the maximal abelian n-extension of k_0 unramified over K. It is therefore the maximal abelian n-extension of L in K^* which is fixed under F (*i.e.* under the action of Gal(L/k_0) 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 $H_k / C'^{1-e_N}_k C_K^{(1-\sigma)\tilde{F}}$ *where* $e_N = n^{-1}\tilde{N}$. Hence the principal genus is the group of ideals with class belonging to $C'^{1-e_N}_k C_K^{(1-\sigma)\tilde{F}}$. From 2.1(ii) this group is included in $P_k I_K^{(1-\sigma)\tilde{F}}$. 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 $C'^{1-e_N}_k$. So $\mathfrak{a}^{(1-\sigma)\tilde{F}}$ is in a class of $C'^{1-e_N}_k$, and the principal genus is indeed $P_k I_K^{(1-\sigma)\tilde{F}}$. The equivalence of the other formulation in (iii) is clear using 2.1(ii).

2.3 COROLLARY. *The genus group of k/k_0 is isomorphic to $N_{k/k_0} I_k / N_{k/k_0} P_k$.*

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

Now if $a \in k_0^\times$ and $a = N_{K/L}\alpha$ then $a = N_{k/k_0}(a/N_{K/k}\alpha^{(n-1)/f})$. Hence:

2.4 LEMMA. *$a \in k_0$ is a norm in k/k_0, if, and only if, it is a norm in K/L.*

For each prime ideal $\mathfrak{p}_i$ ($1 \le i \le t$) of k_0 which is ramified in K/L let $\mathfrak{P}_i$ be a prime of L above $\mathfrak{p}_i$ and for $a \in k_0^\times$ let $\chi_i(a) = \left(\frac{a, K/L}{\mathfrak{P}_i}\right)$ be the norm residue symbol. This yields a map $\chi : k_0^\times \to N^l$ defined by $\chi(a) = (\chi_1(a), \chi_2(a), ..., \chi_l(a))$.

2.5 LEMMA. *$a \in k_0^\times$ is a norm in k/k_0, if, and only if, $a \in \ker\chi$.*

Proof. Suppose $\chi(a) = 1$, *i.e.* $\left(\frac{a, K/L}{\mathfrak{P}_i}\right) = 1$ for $1 \le i \le t$. Then $\left(\frac{a, K/L}{\mathfrak{P}}\right) = 1$ for each conjugate $\mathfrak{P}$ of each prime ideal $\mathfrak{P}_i$ since $\left(\frac{a, K/L}{\mathfrak{P}_i\tau}\right) = \tau^{-1}\left(\frac{a, K/L}{\mathfrak{P}_i}\right)\tau$ for $\tau \in$ G. Therefore a is a local norm for each prime ideal of L ramified in K. So a is a local norm for every completion of K/L because the oddness of n ensures that no infinite valuation is ramified. Thus a is a norm in K/L as the extension is cyclic. So a is a norm in k/k_0 by 2.4. In each case the reverse implication also holds. So a is a norm in k/k_0 if, and only if, $\chi(a) = 1$.

Suppose ${}_NI_k$ is the group of ideals in k which have principal norms in k_0. If $\mathfrak{a} \in {}_NI_k$ and $N_{k/k_0}\mathfrak{a} = (a)$ for $a \in k_0$ then a homomorphism $X : {}_NI_k \to \chi(k_0)/\chi(E_{k_0})$ can be defined by $X(\mathfrak{a}) = \chi(a) \bmod \chi(E_{k_0})$.

2.6 THEOREM. (*cf*. [**6**] & [**7**]) *$\ker X$ is the principal genus of k/k_0.*

Proof. Assume $\mathfrak{a} \in {}_NI_k$ satisfies $N_{k/k_0}\mathfrak{a} = (a)$. 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_0 for some unit ε of k_0 , *i.e.*, if, and only if, $a\varepsilon \in \ker\chi$.

When the class number of k_0 is prime to n the map X can be extended to the whole of I_k. Choose $h \in \mathbb{Z}$ such that $hh_{k_0} \equiv 1 \bmod n$. For $\mathfrak{a} \in I_k$ with $N_{k/k_0}\mathfrak{a}^{h_{k_0}} = (b)$ we must have $X(\mathfrak{a})^n = 1$ and therefore $X(\mathfrak{a}) = X(\mathfrak{a}^{hh_{k_0}}) = \chi(b^h) \bmod \chi(E_{k_0})$. This is consistent with X on ${}_NI_k$ as defined above. Clearly for this extended map $\ker X$ is the group of ideals whose h_{k_0}th power is in the principal genus. Hence:

2.7 THEOREM. *When h_{k_0} is prime to n the n-subgroup of the genus group of k/k_0 is isomorphic to $X(I_k)$.*

2.8 COROLLARY. *When h_{k_0} is prime to n the genus number of k/k_0 divides*

$$\frac{h_{k_0}\prod_{\mathfrak{p}} e_{\mathfrak{p}}}{[E_{k_0} : E_{k_0} \cap N_{k/k_0}k]} .$$

Proof. The factor of the genus number which is prime to n is given precisely by Theorem 2.2(ii). The denominator is the order of $\chi(E_{k_0})$. So it remains to show that $|\chi_i(A)|$ divides the ramification index $e_{\mathfrak{p}_i}$ of $\mathfrak{p}_i$ in K/L where A is the set of all generators of ideals in $(N_{k/k_0}I_k)^{h_{k_0}}$. By Hasse [**8**] II §7, $|\chi_i(A)|$ divides $e_{\mathfrak{p}_i}$ if a is prime to $\mathfrak{p}_i$. Suppose $\mathfrak{p}_i^{h_{k_0}} = (a)$, $\mathfrak{q}_i$ is a prime of k above $\mathfrak{p}_i$ with degree f'_i over k_0, and $\mathfrak{P}_i$ has degree f_i over k_0. Then f_i divides f'_i and $(N_{k/k_0}\mathfrak{q}_i)^{h_{k_0}} = (a^{f'_i})$. Thus, again by Hasse (*op. cit.*), $\mathfrak{q}_i$ gives rise to $\chi_i(a^{f'_i})$ which also has order dividing $e_{\mathfrak{p}_i}$.

Remark. Putting $f = 1$ and using the product formula for norm residue symbols to remove one prime 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 $k_0 = \mathbb{Q}$, $k = \mathbb{Q}(\sqrt[l]{m})$, $L = \mathbb{Q}(\zeta)$, and $K = \mathbb{Q}(\sqrt[l]{m}, \zeta)$. 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 [**13**] these are the prime ideals dividing (m) and, if $m^{l-1} \not\equiv 1 \bmod l^2$, also the prime ideal above (l). Hence:

3.1 THEOREM. *Let* $\mathfrak{a}$ *be an ambiguous ideal of* $k = \mathbb{Q}(\sqrt[l]{m})$. *Then* $\mathfrak{a}^l = (a)$ *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* $m^{l-1} \not\equiv 1 \bmod l^2$, *also the prime l. In the case when* $\mathfrak{a}$ *is principal, a is a norm.*

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

$$(m^{v_p(a)}a^{-v_p(m)})^{(p-1)/l} \equiv 1 \bmod p$$

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

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 $1 \le i \le t$. 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 $p \neq l$ which divide m. Using the properties of Hasse's norm residue and power residue symbols (*see* [**8**] II §11) for the chosen prime $\mathfrak{P}$ in L above $(p) \neq (l)$ one obtains

$$\left(\frac{a, K/L}{\mathfrak{P}}\right) = \left(\frac{a, m}{\mathfrak{P}}\right) = \left(\frac{p, a^{-v_p(m)}m^{v_p(a)}}{\mathfrak{P}}\right) = \left(\frac{a^{v_p(m)}m^{-v_p(a)}}{\mathfrak{P}}\right).$$

Let $n(p) = (p^{f(p)} - 1)/l$ where $f(p)$ is the order of p modulo l. Then $ln(p) = N_{L/\mathbb{Q}}\mathfrak{P} - 1$. 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 $x \in \mathbb{Q}$ prime to p. Thus

$$\left(\frac{a, K/L}{\mathfrak{P}}\right) = 1 \iff (m^{v_p(a)}a^{-v_p(m)})^{n(p)} \equiv 1 \bmod p.$$

This congruence is automatically satisfied when $n(p) \equiv 0 \bmod p-1$, and therefore when l does not divide $p-1$. Otherwise $p \equiv 1 \bmod l$, which gives $n(p) = (p-1)/l$. The theorem now follows.

3.3 COROLLARY. *If* $\mathfrak{a}$ *is an ambiguous ideal of k with* $\mathfrak{a}^l = (a)$ *and a does not satisfy all the congruences of Theorem* 3.2 *then* $\mathfrak{a}$ *is not principal.*

Proof Combine Theorems 3.1 and 3.2.

Let $\{p_i \mid 1 \le i \le t\}$ be the set of ramified primes as described above, and let $\{p_i \mid 1 \le i \le s\}$ be the subset of $p \equiv 1 \bmod l$. Define $\chi_i'(a) = (m^{v_p(a)}a^{-v_p(m)})^{(p-1)/l} \bmod p$ for $p = p_i$ and $1 \le i \le s$. Then $\chi'(a) = (\chi_1'(a), \chi_2'(a), \ldots, \chi_s'(a))$ provides a homomorphism in effect from $\mathbb{Q}^\times$ to $\mathbb{F}_l^s$ where $\mathbb{F}_l$ 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

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

3.4 THEOREM. ker X' *is the principal genus of* $k/\mathbb{Q}$ *and* $|X'(I_k)|$ *is the genus number.*

3.5 THEOREM. (i) *The genus number of* $k/\mathbb{Q}$ *is* l^s, *i.e.* X' *is surjective;*

(ii) *the order of* $X'(I_k^N)$ *is that of the quotient of strongly ambiguous classes by the subgroup of classes corresponding to 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. ([**10**] Lemma 4) $\zeta \in N_{K/L}K$ if, and only if, $p_i^{l-1} \equiv 1 \bmod l^2$ for $1 \le i \le t$ with $p_i \neq l$. Thus for most m every ambiguous class is strongly ambiguous.

Proof. Fröhlich has already proved (i) in [**4**]. Alternatively, (*cf* [**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 $\chi' : \mathbb{Q}^\times \to \mathbb{F}_l^s$ is surjective even when restricted to unramified primes q of order l–1 modulo l. But such primes have prime factors $\mathfrak{q}_1$ and $\mathfrak{q}_{l-1}$ of degree 1 and l–1 respectively in k. So $v(\mathfrak{q}_1) = q$ and $X' = \mathfrak{q}'_0 v$ 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. (*cf* Fröhlich [**4**] Theorem 3). *Let* $l^{s'}$ *be the order of* $X'(I_k^N)$, *and let* $l^{t'}$ *be the number of strongly ambiguous classes. Then* $t' \geq \max(s', t-(l+1)/2)$ *and the class number of* $k = \mathbb{Q}(\sqrt[l]{m})$ *is divisible by*

$$l^{s+t'-s'}.$$

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 $l^{t'-s'}$ classes in the principal genus. The lower bound on t' is just Corollary 1.7(i) with Theorem 3.5(ii).

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

This theorem is given in greater generality, though without proof, by Barrucand and Cohn in [**1**] Theorem 9.1.

References

1. P. Barrucand and 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 and D. Sussman. "The p dimension of class groups of number fields", *J. London Math. Soc.* (2), 2 (1970), 525-529.
3. A. Fröhlich, "The genus field and genus group in finite number fields", I and II, *Mathematika*, 6 (1959), 40-46 and 142-146.
4. A. Fröhlich. "On the l-class group of the field $\mathbf{P}(\sqrt[l]{m})$", *J. London Math. Soc.*, 37 (1962), 189-192.

5. F. Gerth. “On *l*-class groups of certain number fields”, *Mathematika*, 23 (1976), 116-123.
6. R. Gold. “Genera in normal extensions”, *Pacific J. Math*., 63 (1976), 397-400.
7. F. Halter-Koch. “Ein Satz über die Geschlechter relativ-zyklischer Zahlkörper von Primzahlgrad und seine Andwendung auf biquadratisch-bizyklische Körper”, *J. Number Theory*, 4 (1972), 144-156.
8. H. Hasse. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, (Physicia Verlag, Würzburg/Wien, 1970).
9. L. Holzer. “Zur Klassenzahl in reinen Zahlkörpern von ungeraden Primzahlgrade”, *Acta Math*., 83 (1950), 327-348.
10. C. Parry and C. Walter. “The class number of pure fields of prime degree”, *Mathematika*, 23 (1976), 220-226; 24 (1977), 122.
11. C. Walter. “Brauer’s class number relation”, *Acta Arith*., 35 (1979), 33-40.
12. C. Walter. “A class number relation in Frobenius extensions of number fields”, *Mathematika*, 24 (1977), 216-225.
13. U. Wegner. “Zur Theorie der auflösbaren Gleichungen von Primzahlgrad”, *J. f. reine u. angew. Math*., 168 (1932), 176-190.
14. 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: *ALGEBRAIC NUMBER THEORY: global fields*; *metabelian extensions*.

Received on the 23rd of January, 1979.