TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 277, Number 1, May 1983

RELATIVE GENUS THEORY AND THE CLASS GROUP OF l-EXTENSIONS[1]

BY

GARY CORNELL

ABSTRACT. The structure of the relative genus field is used to study the class group of relative l-extensions. Application to class field towers of cyclic l-extensions of the rationals are given.

Given a number field E one tries to understand the unramified abelian extensions of E and so by Class Field Theory derive information about the class group of E, C_E. One way of doing this is to ask for the maximal abelian unramified extension of E of the form EF_* where F_* is an abelian extension of $F \subset E$. This field is called the relative genus field and we denote it by E_F^*. If $F = Q$ we speak of the absolute genus field. This paper will use relative genus theory to study the class group of certain l-extensions of Q. (Henceforth, l will always be an odd prime.) In particular we give applications to class field towers of such fields. We also study the l-ranks of the class group of number fields E containing a cyclic subextension of degree l. This will lead to a slight improvement on a bound of Iwasawa [**13**]. This technique is then used to give bounds on both the l-rank and the order of the class group of elementary abelian l-extensions of Q.

We let H_E (respectively $H_E^{(l)}$) denote the Hilbert class field of E (respectively the l-Hilbert class field). Also we refer simply to the l-class rank to mean the l-rank of the class group.

PROPOSITION 1. *Let E/F be normal and F_* the fixed field of the commutator subgroup of* $\mathrm{Gal}(H_E/F)$. *Then $E_F^* = EF_*$.*

PROOF. Any abelian extension of F whose composite with E is contained in H_E is contained in F_*. Since F_*E is contained in the tower $E \subset F_*E \subset H_E$, it is unramified over E. The result follows.

PROPOSITION 2. *Suppose E/F is normal and both fields are normal over some subfield L of F. Then E_F^* is also normal over L.*

PROOF. We know H_E/L is Galois and $\mathrm{Gal}(H_E/F)$ is a normal subgroup of this group. The commutator subgroup of $\mathrm{Gal}(H_E/F)$ is a characteristic subgroup of

Received by the editors February 26, 1982 and, in revised form, May 25, 1982.

1980 *Mathematics Subject Classification*. Primary 12A65; Secondary 12A50.

[1] This paper is based on an improved version of part of the authors Ph.D. thesis at Brown University written under the direction of Professor M. Rosen. Support has been graciously provided by the Vaughn Foundation.

$\mathrm{Gal}(H_E/F)$, hence normal in $\mathrm{Gal}(H_E/F)$ because characteristic subgroups of normal subgroups are normal. This implies that F_*, the fixed field of this commutator subgroup, is also normal. So $E_F^* = EF_*$ is the composite of two normal extensions of L and so is normal over L.

PROPOSITION 3. *Suppose E/F is cyclic with generator σ. Then $\mathrm{Gal}(E_F^*/E) \approx C_E/C_E^{1-\sigma}$ under the Artin-map.*

PROOF. Since E/F is abelian we know the commutator subgroup of $\mathrm{Gal}(H_E/F)$ is contained in $C_E \approx \mathrm{Gal}(H_E/E)$. We also know that $\langle \sigma \rangle$ acts on C_E by conjugation. Given any commutator $aba^{-1}b^{-1}$ with $a = \alpha x$, $b = \beta y$, $\alpha, \beta \in \langle \sigma \rangle$, $x, y \in C_E$ (where we regard $\langle \sigma \rangle$ as being lifted to $\mathrm{Gal}(H_E/F)$) then

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} = x^{\alpha} \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \\ &= x^{\alpha}(yx^{-1})^{\alpha\beta}(\alpha\beta)\alpha^{-1}y^{-1}\beta^{-1} = x^{\alpha}(yx^{-1})^{\alpha\beta}(y^{-1})^{\beta}, \end{aligned}$$

where, as usual, $(\ \ )^{\alpha} = \alpha(\ \ )\alpha^{-1}$ and the manipulations are permissible since both C_E and $\langle \sigma \rangle$ are abelian. This is in $C_E^{1-\sigma}$ since α, β are powers of σ. Conversely, by choosing $\beta = 1$, $\alpha = \sigma$ we get the reverse inclusion.

We will often be applying the preceding proposition to the following exact sequence:

$$(*) \qquad 0 \to C_E^G \to C_E \to C_E \to C_E/C_E^{1-\sigma}, \qquad G = \langle \sigma \rangle.$$

(C_E^G is usually called the group of ambiguous ideal classes and $C_E/C_E^{1-\sigma}$ the genus group.) So, for example, we get the following

PROPOSITION 4. *The ambiguous ideal class group has the same order as the degree E_F^*/E.*

PROOF. This follows from the fact that the alternating product of the orders of the groups in $(*)$ is one and that $\mathrm{Gal}(E_F^*/E) \approx C_E/C_E^{1-\sigma}$.

REMARK. From now on if it is clear from the context, we will suppress the subscript of C_E.

The groups C^G and $C/C^{1-\sigma}$ are not obviously isomorphic. This is true, however, when E is a cyclic extension of Q of degree l, since both are easily seen to be elementary abelian l-groups. I do not know if these groups can be nonisomorphic or, alternately, if nontrivial conditions can be given to force them to be isomorphic.

LEMMA. *If $G = \langle \sigma \rangle$ is a cyclic group of order l and A is a G-module such that the norm element $1 + \sigma + \cdots + \sigma^{l-1}$ annihilates A, then $A^l = \{x^l \mid x \in A\} = A^{(1-\sigma)^{l-1}}$.*

PROOF. The hypothesis implies that A is a $Z[G]/1 + \sigma + \cdots + \sigma^{l-1}$ module, i.e. a module over $Z[\mu_l]$ where μ_l is a primitive lth root of 1. Since the ideal $(l) = (1 - \mu_l)^{l-1}$ and σ acts as μ_l, the result follows.

We will denote by $r_l(A)$ the l-rank of an abelian group A. It is, for example, $\dim_{F_l}(A/A)^l$.

Proposition 5. *Let A be a G-module where G is a cyclic group of order l, generated by σ. Then*:

(i) $r_l(A) \leqslant (l) r_l(A/A^{1-\sigma})$.

(ii) *If the norm annihilates then* $r_l(A) \leqslant (l-1) r_l(A/A^{1-\sigma})$.

(iii) *Again assuming the norm annihilates, suppose A contains an element of order l^2, then* $r_l(A) \geqslant l-1$.

Proof. Consider the series of surjective maps

$$\cdots \to A^{(1-\sigma)^i}/A^{(1-\sigma)^{i+1}} \to A^{(1-\sigma)^{i-1}}/A^{(1-\sigma)^i} \to \cdots$$

given by $\bar{a} \to \bar{a}^{1-\sigma}$. Under the hypothesis for both (ii) and (iii) the previous lemma implies that $A^{(1-\sigma)^{l-1}} = A^l$. Thus (ii) follows by noticing the filtration has $(l-1)$ steps and each one has, by the surjectivity rank, less than that of $A/A^{1-\sigma}$; (iii) also follows because each of the steps has rank at least one since the existence of an element of order l^2 implies that $A^{(1-\sigma)^l}/A^{(1-\sigma)^{l-1}}$ is nontrivial. For (i) the module $A^{1-\sigma}$ is annihilated by the norm, so the previous proposition applies. Thus $A^{(1-\sigma)^l} = (A^{(1-\sigma)})^{l-1} = (A^{1-\sigma})^l \subset A^l$. So there is a surjective map $A/A^{(1-\sigma)^l} \to A/A^l$. Since $r_l(A) \geqslant r_l(A/A^{(1-\sigma)l}) \geqslant r_l(A/A^l) = r_l(A)$, we have $r_l(A) = r_l(A/A^{(1-\sigma)^l})$. The result now follows as in the proof of (ii), except now we have an l-step filtration.

Remark. The preceding is due to Inaba [**11**]. For another approach see [**5**].

Theorem 1. *Suppose E/F is abelian with t ramified primes, $t \geqslant 1$. Then E_F^* may be obtained by composing E with a ramified extension of F having at most $t-1$ ramified primes.*

Proof. E_F^*/F is abelian so we can take the inertia group $T_{\mathfrak{p}}$ for any prime $\mathfrak{p}$ of F. Its fixed field L has at most $t-1$ ramified primes. We claim $EL = E_F^*$. E_F^*/EL is totally ramified since EL is included in the tower $L \subset EL \subset E_F^*$ and E_F^*/L is totally ramified. It is also unramified as it is included in the tower $E \subset EL \subset E_F^* \subset H_E$. Thus the degree E_F^*/EL is one and so $E_F^* = EL$.

Remark. It is easy to construct examples where L has $< t-1$ ramified primes.

Corollary 1 (Iwasawa [**12**]). *Suppose E/F is a Galois l-extension with only one ramified prime, and that is totally ramified. Then $l \mid h_E \Leftrightarrow l \mid h_F$.*

Proof. Since every l-group has a chain of subgroups, each normal and of index l in the next, we can assume E/F is cyclic of degree l. Then $l \mid h_E \Leftrightarrow C_E^{(l)}$ is nontrivial $\Leftrightarrow$ the group C_E has nontrivial ambiguous ideal classes (i.e. $(C_E^G)^{(l)}$ is nontrivial). By Proposition 4 this is so if and only if l divides the degree E_F^*/E. Now Theorem 1 says E_F^* can be gotten by composing E with an unramified extension of F. Since E is totally ramified it is disjoint from any unramified extension of F. Thus l must divide h_F.

Corollary 2 (Kiselevsky [**14**]). *Suppose* $\mathrm{Gal}(E/F) = G$ *is a cyclic unramified extension of degree n. Then* $|C_E^G| = |C_F|/n = h_F/n$.

PROOF. Again by the exact sequence $(*)$, $|C_E^G|=|C_E/C_e^{1-\sigma}|$. The latter, by Proposition 4, equals $|E_F^*:E|$. Since $E_F^*=EH_F=H_F$, the degree of $|E_F^*:E|=h_F/n$.

THEOREM 2. *Suppose E/F is cyclic of degree l with $t\geqslant 1$ ramified primes. Then $r_l(C_E)\leqslant l(t-1+r_l(C_F))$. If E/F is unramified then $r_l(C_E)\leqslant l(r_l(C_F))$. Finally, if $l\nmid h_F$ then $r_l(C_E)\leqslant (l-1)(t-1)$.*

PROOF. Let $p_1,\dots,p_t$ be the primes that ramify. Theorem 1 says $E_F^*=EL$ where L has at most $t-1$ ramified primes. Thus in L the group T generated by the inertia groups of the primes that ramify have rank at most $t-1$. The fixed field of T is an unramified abelian extension of F and so has rank at most $r_l(C_F)$. Thus $r_l(\mathrm{Gal}(L/F))\leqslant t-1+r_l(C_F)$. So $\mathrm{Gal}(EL/E)=\mathrm{Gal}(E_F^*/E)$ has rank also $\leqslant (t-1)+r_l(C_F)$. But again by Proposition 4 this group is isomorphic to $C_E/C_E^{1-\sigma}$. The proof now follows by applying part (i) of Proposition 5. If $l\nmid h_F$ then we apply part (ii) of this proposition. If there are no ramified primes, part (i) still applies since $\mathrm{Gal}(E_F^*/E)$ has rank $\leqslant r_l(C_F)$. (This is a slight improvement on a result in Iwasawa [**13**].)

We can use Theorem 2 to derive bounds on the l-rank of C_E in terms of the l-rank of C_F whenever E/F is a Galois l-extension. This is because any l-group has at least one normal subgroup of every index and so we have only to proceed by induction in towers. However, this procedure depends on the choice of the sequence of fields $F=F_0\subset\cdots\subset F_n=E$. In one case though there is a canonical choice of fields.

THEOREM 3. *Suppose E/Q is an elementary abelian extension of degree l^n having n-ramified primes. Then $r_l(C_E)\leqslant (l^{n-1})(l-1)(n-1)=\phi(l^n)(n-1)$, where ϕ is the Euler totient function.*

PROOF. Since the number of ramified primes is the same as the rank, $\mathrm{Gal}(E/Q)$ must be the direct sum of the inertia groups T_{p_i}, $1\leqslant i\leqslant n$. Thus we can choose a subgroup of index l disjoint from all the T_{p_i}. The fixed field F of this group is a cyclic extension of degree l of Q having n-ramified primes, so by Theorem 2 we know that $r_l(C_F)\leqslant (l-1)(n-1)$. Now E/F is an unramified abelian extension of degree l^{n-1} since $\mathrm{Gal}(E/F)$ has been chosen to be disjoint from the T_{p_i}. The theorem now follows by applying Theorem 2 $n-1$ times.

It is tempting to conjecture that similar bounds hold for all elementary abelian l-extensions and not just those of the special type above. I do not know if this is reasonable. At least it is of the right order of magnitude as shown by the following weaker result: Suppose $E=F_n\supset F_{n-1}\supset\cdots\supset F_0=F$ is a chain of fields with each F_{i+1}/F_i cyclic of degree with t_i ramified primes. Set $e_i=t_i$ if $t_i\geqslant 1$ and $e_i=1$ if $t_i=0$. Then

THEOREM 4. $r_l(C_E)\leqslant \sum_{i=1}^{n-1} l^{n-i}(e_i-1)+l^n r_l(C_F)$. *If $l\nmid h_{F_0}$ then*

$$r_l(C_E)\leqslant \sum_{i=0}^{n-1} l^{n-i}(e_i-1)-l^{n-1}(e_0-1).$$

PROOF. Both are easy inductions using Theorem 2.

REMARKS. If $F_0 = Q$ we can choose each t_i to be at least one but this does not always give the best bounds. Exactly how good these bounds are is less clear, since this involves proving the existence of fields having large l-class rank. For example, in the case $F_0 = Q$ we know the rank is $\leqslant (l-1)(t-1)$ for cyclic extensions F_1 of degree l, but nothing is known if ranks larger than $2(t-1)$ can be obtained. That the rank can be $t-1$ exactly is a theorem of Gerth [**8**], that ranks $2(t-1)$ can be obtained follows from the early work of Fröhlich but does not appear to have explicitly occurred in print. Exactly which (if any) ranks $> 2(t-1)$ can be obtained from the work of Fröhlich is unclear.

For arbitrary elementary abelian extensions of Q in a subsequent paper, following a suggestion of T. Takeuchi, improving on the results of [**1**], we can prove that extensions of Q of type $(Z/l)^n$ can have l-class rank $\geqslant (l^n - 1)/(l-1) - n$. This shows Theorem 3 is at least in the right ballpark. Also it is worth noting that lower bounds (at least in the tamely ramified case) of $(n)(n-1)/2 - n$ were obtained in [**5**] following ideas implicit in the work of Furuta and Fröhlich.

We can combine the above two theorems with the following elementary observation to derive information on the order of the l-class group of an elementary abelian l-extension of Q. (It is worth pointing out that prime to l, part of the class group is the direct sum of the corresponding parts of the fields on the first layer. For this result (which has been proved repeatedly) see [**16**].)

Let G be a finite group. G is decomposable if there exists a partition of G by subgroups H_i such that $G = \bigcup H_i$ with the intersection of the H_i's being only the identity. A complete classification of such groups is available, see [**9**]. However, it is obvious that an elementary abelian l-group admits such a decomposition by the subgroups of order l. Corresponding to a decomposition we have an equation in the integral group ring $Z[G]$. Set $N_H = \Sigma_{\sigma \in H}\sigma$. Then $N_G = \Sigma_H N_H - (\#H - 1)$ where $\#H$ is the number of subgroups in the decomposition. In the special case when $G \approx Z/l \times Z/l$, we have for any G-module A, $A^l A^{N_G} = \Pi A^{N_H}$, since there are $l+1$ subgroups of order l. Thus, if A is the l-class group of a bicyclic extension of Q of type (l, l), where the norm of course annihilates the class group, we have $|A^l| \leqslant \Pi |A_H|$ where A_H is the l-class group of the cyclic extension of Q fixed by H. Now $|A| = |A^l||A/A^l|$ and the number $|A/A^l| = l^{r_l(A)}$ is bounded by the previous discussion. So proceeding by induction we can bound the l-class number in any elementary abelian extension in terms of the l-class numbers of the first layers.

Now we want to give examples where $E_F^* \supsetneqq EH_F$. We have the following theorem of Furuta [**6**] for the degree E_F^*/E:

$$|E_F^* : E| = \frac{h_F \cdot \Pi e_{\mathfrak{p}}'}{|E_0 : F||\varepsilon : \eta|},$$

where h_F is the class number of F, $e_{\mathfrak{p}}'$ is the ramification in the maximal abelian subfield of the completion of E at $\mathfrak{p}$ over the completion of F, E_0 is the maximal subfield of E abelian over F and $|\varepsilon : \eta|$ is the index of the units which are everywhere local norms in the full group of units.

The difficulty with the above formula is that the presence of the unit index makes it difficult to decide when this number is > 1. Of course one can always take fields having enough primes ramified and for those fields it can be shown that $|E_F^* : E| > h_F$. These proofs more or less depend on the unit group being finitely generated. What we want to do is describe a set of primes of positive density such that if $E | F$ has ramification in this set it is "quite likely" that the genus field is properly larger than $H_F E$. We will then use this to prove the existence of l-extensions of Q whose class groups are particularly interesting.

Class Field Theory says the maximal tamely ramified abelian extension of a number field F at a prime $\mathfrak{p}$ (to be denoted by $F^{\mathfrak{p}}$) is the full ray class field with conductor $\mathfrak{p}$. It is of finite degree over H_F, the Hilbert class field of F, and in the tower of fields $F \subset H_F \subset F^{\mathfrak{p}}$ the Galois groups correspond to the short exact sequence

$$(**) \qquad 0 \to (\mathfrak{O}/\mathfrak{p})^*/U/U^1(\mathfrak{p}) \to I_{\mathfrak{p}}/p_{\mathfrak{p}} \to C_F \to 0$$

where $\mathfrak{O}$ is the ring of integers in F, U (respectively $U^1(\mathfrak{p})$) are the units of F (respectively the unity $\equiv 1(\mathfrak{p})$), $I_{\mathfrak{p}}$ is the group of fractional ideals prime to $\mathfrak{p}$, and $P_{\mathfrak{p}}$ is the principal ideals which have a generator congruent (multiplicatively) to 1 mod $\mathfrak{p}$ and C_F is the class group of F.

REMARK. Since the exact sequence $(**)$ need not split, it is of interest to study exactly what is the structure of the group $I_{\mathfrak{p}}/P_{\mathfrak{p}}$. Both the splitting and nonsplitting of $(**)$ can occur and both have interesting consequences (see **[4]** for more on this). For our purposes it will be enough to show that, for a certain set of primes of positive density, the group $(\mathfrak{O}/\mathfrak{p})^*/U/U^1(\mathfrak{p})$ is large. Notice that this is not a priori obvious because $U/U^1(\mathfrak{p})$ can be large even while $(\mathfrak{O}/\mathfrak{p})^*$ is.

Let L be the extension of F gotten by adjoining to F the nth roots of all the units of F. By Dirichlet's unit theorem this is a finite extension of F containing the nth roots of 1.

THEOREM 5. *If p is any prime from Q which splits completely in L then*

$$n \,\Big|\, \frac{(\mathfrak{O}/\mathfrak{p})^*}{u/u'(\mathfrak{p})}$$

for any $\mathfrak{p}$ above p in F.

PROOF. By construction the completion of F at $\mathfrak{p}$ is Q_p and, moreover, the polynomial $X^n - u$ splits completely in $Q_p = F_{\mathfrak{p}} = L_{\mathfrak{p}}$. Thus every global unit is locally an nth power. Moreover, since L contains the nth roots of 1 and p splits completely in L, we have $p \equiv 1$ (n). So $N_{\mathfrak{p}} = |(\mathfrak{O}/\mathfrak{p})^*| = p$ is also $\equiv 1$ (n). Set $\Gamma = (\mathfrak{O}/\mathfrak{p})^*$. Then by the above, $u/u'(\mathfrak{p})$ maps entirely into Γ^n. The result now follows since, for any finite abelian group with $n \,|\, |\Gamma|$, the index of Γ^n in Γ is at least n.

We will denote the set of all primes in F that satisfy the conditions of Theorem 5 by $\Omega_n(F)$. Notice that if p is any prime of Q below a prime in $\Omega_n(F)$, the ray class field of F with conductor p (considered as an integral ideal of F) has large n-rank ($=$ numbers of summands in the Galois group of F^p/F whose order is divisible by

n). More precisely, the rank is at least $|F:Q|$ and may be larger depending on whether $n \mid h_F$ and the sequence (**) splits. To return to the problem of forcing $|E_F^*:E|$ large, we must construct unramified abelian extensions of E. The easiest way is to use

Abhyanker's Lemma. *Let E_1, E_2 be Galois extensions of a number field F. Suppose a prime $\mathfrak{p}$ of F is tamely ramified in E_2 with ramification index e_2. Suppose $\mathfrak{p}$ is also ramified in E_1 with ramification index e_1. Suppose that $e_2 \mid e_1$. Then $E_2E_1 \mid E_1$ is unramified at $\mathfrak{p}$.*

For a proof see [**2** or **3**].

We now want to construct cyclic extensions F of Q of degree l having infinite l-class field tower. If we naively apply the Golod-Shafarevich bound then the l-rank of the class group must be $\geqslant 2 + 2\sqrt{\Gamma_F + \delta_F}$, where Γ_F is the number of infinite primes in F and $\delta_F = 0$ or 1 according as the lth roots of 1 are in F. Then one applies the fact that the rank of the class group is at least $t - 1$, where t is the number of ramified primes, to conclude that there are fields having infinite class field towers. In [**1**], on which this paper is based, it was shown that there exist infinitely many cyclic extensions of Q of degree l having only four ramified primes which, nonetheless, have infinite l-class field towers. Then T. Takeuchi remarked in a letter to the author that a theorem of Furuta [**7**] enables one to replace this (for $l \geqslant 13$) by only two ramified primes and by three ramified primes for all odd l. Since the methods are slightly different we will give both results here. For Takeuchi's version, which was done independently, see [**15**].

Choose any prime $p_1 \equiv 1\ (l)$ and let k_1 be the unique cyclic extension of Q of degree l having only p_1 ramified. Choose p_2, p_3, p_4 below primes in $\Omega_l(k_1)$. Let K be any field cyclic of degree l over Q having p_1, p_2, p_3, p_4 ramified.

Theorem 6. *K has an infinite l-class field tower.*

Proof. Kk_1 is, by Abhyanker's Lemma, an unramified abelian extension of K of degree l. We will show that Kk_1 has an infinite l-tower which implies that K itself does. Since $|Kk_1:Q| = l^2$ the Golod-Shafarevich bound says Kk_1 has infinite l-class field towers whenever $r_l(C_{Kk_1}) \geqslant 2 + 2\sqrt{l^2 - 1}$. We will explicitly construct an unramified abelian extension Q having l-rank larger than this. So this, by class field theory, implies that the rank of C_{Kk_1} is also $\geqslant 2 + 2\sqrt{l^2 - 1}$. Let F be the maximal elementary abelian l-extension in the ray class field of k_1 with conductor $p_2p_3p_4$. Since we have chosen p_2, p_3, p_4 in $\Omega_l(k_1)$, this has l-rank at least $3l$ (and in fact since $l \nmid h_{k_1}$, exactly $3l$). Moreover, the ramification index of any prime above p_i, $i = 2, 3, 4$, is exactly l. Thus Abhyanker's Lemma implies that FKk_1 is an unramified abelian l-extension of Kk_1 of rank at least $3l - 1$ (and actually it equals $3l - 1$ since Kk_1 is in F). This finishes the proof since $3l - 1 \geqslant 2 + 2\sqrt{l^2 - 1}$ for all odd l.

Now the improvement of this result will depend on a remarkable theorem of Furuta that in some circumstances enables us to replace "large unramified abelian l-extensions" by "large abelian l-extensions". We will state the theorem only in the tamely ramified case where it is somewhat simpler.

THEOREM (SEE THEOREM 3 IN [7]). *A number field E admits an infinite l-class field tower if E contains a subfield L such that E/L is a Galois l-extension (i.e. the degree is a power of l) and such that the l-rank of the maximal abelian l-extension E_0 of L in E has l-rank $\geqslant 2 + 2\sqrt{\rho + \tau + 1}$, where ρ is the rank of the units of L modulo lth powers and τ is the number of primes of L which ramify.*

Using this theorem we need only choose one prime $p_1 \equiv 1\ (l)$ and p_2 any prime in $\Omega_l(k_1)$ where, as before, k_1 is the unique cyclic extension of Q having only p_1 ramified. Let K now be any field cyclic over Q of degree l with both p_1, p_2 ramified. We claim K has an infinite l-class field tower. As before it is enough to prove that Kk_1 has an infinite class field. Let F now be the maximal elementary abelian l-extension in the ray class field of k_1 with conductor p_2. As before $F \supset Kk_1$ and is an unramified abelian extension of it. We apply Furuta's theorem to the pair F/k_1 to conclude F has an infinite l-class field tower. This implies that Kk_1 does, which in turn implies that K does. In Furuta's theorem ρ is $l - 1$ since k_1 is of degree l, l-odd, and so the lth roots of 1 are not in k_1. τ is l since all the primes above p_2 ramify. Now for $l \geqslant 13$, $l - 1 \geqslant 2 + 2\sqrt{(l-1) + \tau + 1}$, so the result follows.

REMARKS. The extension F/K while unramified is not abelian. In fact, it is easy to see that Gal(F/Q) is a wreath product of $(Z/l)^l$ by Z/l. Such groups have no large abelian subquotients. Thus we cannot use F to get fields K having very large l-class rank. However, we can apply Burnside's basis theorem to conclude the following:

THEOREM 7. *The l-rank of C_K is at least 2, and C_K contains nonambiguous ideal classes.*

PROOF. If the l-rank is at least two then C_K must contain ambiguous ideal classes. This is because K has only two ramified primes over Q and so the rank of the ambiguous ideal classes is one. So it is enough to prove the first statement.

Since F/Q is Galois, F/K is also. Since it contains Gal(F/Kk_1) which is of rank $l - 1$, it is not cyclic. Thus Burnside's basis theorem implies Gal(F/K) has an elementary abelian quotient of rank 2. Since (as remarked before) F/K is unramified, we are done.

REMARK. This gives another solution to the problem solved by Gras in his thesis [**10**].

As a final theorem we give an amusing consequence of Proposition 5 to infinite class field towers.

THEOREM 8. *Suppose $l \geqslant 11$ and K is a cyclic extension of Q of degree l having an element of order l^2 in the class group. Then K has an infinite l-class field tower.*

PROOF. By Proposition 5 we know the l-rank of C_K is then at least $l - 1$. Since the Golod-Shafarevich bound for a cyclic extension of odd degree l is $\geqslant 2 + 2\sqrt{l-1}$, it is easy to check that, for all $l \geqslant 11$, $l - 1$ is indeed larger than this.

REMARK. Unfortunately, we do not know if there exist infinitely many cyclic extensions of Q of degree l having elements of order l^2 in the class group. This does not even seem to be known for $l = 3$. For $l = 2$ it is true but the proofs do not seem to generalize.

BIBLIOGRAPHY

1. G. Cornell, *Genus fields and the class group of number fields*, Ph.D. Thesis, Brown University, 1978.

2. ______, *Abhyankar's lemma and the class group*, Number Theory, Carbondale, 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979) (M. Nathanson, ed.), Lecture Notes in Math., vol. 751, Springer-Verlag, Berlin and New York, pp. 82–88.

3. ______, *On the construction of relative genus fields*, Trans. Amer. Math. Soc. **271** (1982), 501–511.

4. ______, *Structure of the ray class group and the class group* (to appear).

5. G. Cornell and M. Rosen, *Cohomological analysis of the class group extension problem* (Proc. Conf. Number Theory, Queen's Univ., New York) (P. Ribenboim, ed.), Kingston, 1980, pp. 287–308.

6. Y. Furuta, *The genus field and genus number in finite number fields*, Nagoya Math. J. **29** (1967), 281–285.

7. ______, *On class field towers and the rank of ideal class groups*, Nagoya Math. J. **48** (1972), 145–157.

8. F. Gerth, *Number fields with prescribed l-class groups*, Proc. Amer. Math. Soc. **49** (1975), 284–288.

9. D. Gorenstein (Editor), *Reviews on finite group theory*, Amer. Math. Soc., Providence, R.I., 1974.

10. G. Gras, *Sur les l-classes d'ideaux dans les extensions cycliques relatives de degreé premier l*, Ann. Inst. Fourier (Grenoble) **29** (1973), 1–49.

11. E. Inaba, *Über die structur der l-Klassengruppe Zahlkörper von primzahlgrad l*, J. Fac. Sci. Univ. Tokyo Sect. II **21** (1940), 61–115.

12. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 189–192.

13. ______, *On the μ-invariants of Z_l-extensions*, Number Theory, Algebraic Geometry and Commutative Algebra (in honor of Y. Akizuki), Kinokuniya, Tokyo, 1973, pp. 1–11.

14. H. Kisilevsky, *Some results related to Hilbert's Theorem* 94, J. Number Theory **2** (1970), 199–206.

15. T. Takeuchi, *Notes on class field towers of cyclic fields of degree l*, Tôhoku Math. J. **31** (1979), 301–307.

16. C. Walters, *Brauer's class number relation*, Acta Arith. **35** (1979), 33–40.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CONNECTICUT, STORRS, CONNECTICUT 06268