COMPOSITIO MATHEMATICA

GARY CORNELL
MICHAEL I. ROSEN

The ℓ-rank of the real class group of cyclotomic fields

Compositio Mathematica, tome 53, n° 2 (1984), p. 133-141
<http://www.numdam.org/item?id=CM_1984__53_2_133_0>

Compositio Mathematica 53 (1984) 133–141.

THE ℓ-RANK OF THE REAL CLASS GROUP OF CYCLOTOMIC FIELDS

Gary Cornell * and Michael I. Rosen **

Introduction

Let K_m for m not congruent to 2 modulo 4 denote the m'th cyclotomic field, i.e. $K_m = \mathbb{Q}(e^{(2\pi i)/m})$. Let K_m^+ denote the maximal real subfield of K_m, and h_m^+ and h_m the respective class numbers. Finally, let ℓ be a prime number. We will be concerned with the question of when $\ell | h_m^+$. This is of interest since h_m^+ is not easily calculated. It is especially interesting to determine when $2 | h_m^+$ as this is related to certain questions concerning the actions of groups on spheres. For more information on this see Section 2c of *S.* Lang's article [9].

In this paper we prove, among other things, the following two theorems.

THEOREM A: *If m is divisible by five or more primes then $2 | h_m^+$.*

THEOREM B: *If ℓ is an odd prime and if m is divisible by four or more primes congruent to* 1 *modulo ℓ then $\ell^2 | h_m^+$.*

We, in fact, prove much more detailed and precise results, but these are more cumbersome to state. In particular, we are able to partially deal with the cases where fewer primes of the requisite type divide m. Unfortunately our methods yield nothing when m is prime.

When m is divisible by many primes, stronger results than those given here have been obtained by D. Kubert [8] for the case $\ell = 2$, and by G. Cornell [1] in general. Kubert uses the theory of cyclotomic units and the Stickelberger ideal, Cornell the theory of relative genus fields. The methods used here are based on a cohomological approach which goes back to early work of A. Fröhlich [2,3] and a paper of Y. Furuta [4]. A more recent paper by M. Razar [11] contains related material. These methods, in addition to being relatively elementary, have the advantage

* Partially supported by a grant from the Vaughn Foundation.
** Partially supported by a grant from the National Science Foundation.

of yielding stronger results that those of Kubert and Cornell when m is divisible by "few" primes.

We wish to thank the referee for pointing out an error in earlier versions of this paper and for suggesting a number of improvements. In particular Lemma 1 of Section 2 and Proposition 7 of the appendix are due to the referee.

Section 1: Preliminaries

Let L/K be a finite extension of algebraic number fields and J_L the idele group of L. We define two groups $A(L/K) = K^* \cap N_{L/K}J_L/N_{L/K}L^*$ and $B(L/K) = E_K \cap N_{L/K}J_K/E_K \cap N_{L/K}L^*$. Here E_K denotes, as usual, the unit group of K. Both these groups occur in the study of obstructions to the Hasse norm theorem. For example, see Garbanati [5], Gerth [6], and Razar [11]. When L/K is Galois, Furuta shows $A(L/K)/B(L/K)$ is isomorphic to the Galois group of the central class field over the genus field (with respect to the extension L/K). The following proposition shows directly how this quotient group is related to the structure of the class group C_L of L.

PROPOSITION 1: *C_L has a subquotient isomorphic to $A(L/K)/B(L/K)$.*

PROOF: Let $U_L \in J_L$ and $U_K \subset J_K$ be the respective groups of unit ideles. Consider the diagram

$$\begin{array}{ccccccc} (1) & \to & U_L L^* & \to & J_L & \to & C_L \to (1) \\ & & \downarrow & & \downarrow & & \downarrow \\ (1) & \to & U_K K^* & \to & J_K & \to & C_K \to (1) \end{array}$$

where the vertical arrows are given by norm maps. The snake lemma yields an exact sequence

$$ {}_N C_L \to U_K K^*/N(U_L L^*) \to J_K/NJ_L$$

where $N = N_{L/K}$ and ${}_N C_L$ is the subgroup of the class group annihilated by the norm. If follows that ${}_N C_L$ maps onto $U_K K^* \cap NJ_L/N(U_L L^*)$. Since $NU_L \subseteq U_K$, it follows that C_L has a subquotient isomorphic to $K^* NU_L \cap NJ_L/N(L^* U_L)$. It is now an easy exercise to show this latter group is isomorphic to $A(L/K)/B(L/K)$. For details see page 151 of [4].

When L/K is not Galois the group $A(L/K)$ seems difficult to understand. However, when L/K is Galois, we have the following important result due to John Tate. A proof can be found on page 198 of Cassels-Fröhlich, Algebraic Number Theory (Thompson Book Company, Washington, D.C., 1967).

THEOREM: *If L/K is Galois with group G, then $A(L/K)$ is isomorphic to $H^{-3}(G, \mathbb{Z})$ modulo the subgroup generated by the images of all the $H^{-3}(G^v, \mathbb{Z})$ under corestriction. Here v runs through all the primes finite and infinite of K, and G^v is the decomposition group of some fixed prime of L above v.*

We can now state and prove one of our principal results.

PROPOSITION 2: *Let $L/\mathbb{Q}$ be an abelian ℓ-extension of the rationals with Galois group G. Assume the inertia group of 2 is cyclic. If G is the direct sum of t cyclic groups and s finite primes of $\mathbb{Q}$ ramify in L then the ℓ-rank of C_L, $r_\ell C_L$, satisfies*

$$r_\ell C_L \geqslant \frac{t(t-1)}{2} - s - e$$

where $e = 1$ if -1 is a local norm everywhere but not a global norm, and is zero otherwise. Note $e = 0$ if ℓ is odd.

PROOF: By Proposition 1 it suffices to consider $A(L/K)/B(L/K)$. It is easy to see that e is the ℓ-rank of $B(L/K)$. Thus we concentrate on $A(L/K)$.

Write $G \approx C_1 \oplus C_2 \oplus \ldots \oplus C_t$, where the C_i are cyclic. By a well known "universal coefficient" theorem (see, for example, Yamazaki [12]) we have, with $\mathbb{Q}/\mathbb{Z}$ acted on trivially,

$$H^2(G, \mathbb{Q}/\mathbb{Z}) \approx \bigoplus_{i=1}^{t} H^2(C_i, \mathbb{Q}/\mathbb{Z}) \oplus \bigoplus_{i<j} \operatorname{Hom}(C_i \otimes C_j, \mathbb{Q}/\mathbb{Z}).$$

For each i, $H^2(C_i, \mathbb{Q}/\mathbb{Z})$ is zero, and for each $i < j$, $\operatorname{Hom}(C_i \otimes C_j, \mathbb{Q}/\mathbb{Z})$ is cyclic. Thus, $r_\ell H^2(G, \mathbb{Q}/\mathbb{Z}) = t(t-1)/2$.

By duality, $H^{-3}(G, \mathbb{Z}) \approx H^3(G, \mathbb{Z})$. This together with the exact sequence $(0) \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to (0)$ shows $H^{-3}(G, \mathbb{Z}) \approx H^2(G, \mathbb{Q}/\mathbb{Z})$.

Finally, we need to consider $H^{-3}(G^v, \mathbb{Z}) \approx H^2(G^v, \mathbb{Q}/\mathbb{Z})$. If v is unramified or infinite G^v is cyclic and so $H^2(G^v, \mathbb{Q}/\mathbb{Z})$ is trivial. If v is ramified and finite the inertia group T^v is cyclic. For v above 2 this follows by hypothesis whereas for v dividing an odd prime it follows from the fact that L is an abelian extension of $\mathbb{Q}$. Since G^v/T^v is also cyclic the ℓ-rank of G^v is at most 2 and so $r_\ell H^2(G^v, \mathbb{Q}/\mathbb{Z})$ is at most 1. From Tate's theorem we conclude that $r_\ell A(L/K) \geqslant [t(t-1)/2] - s$. This completes the proof.

We remark that variants of Proposition 2 are easy to obtain by this method. For example, if each C_i were cyclic of order ℓ^a we could obtain a result about the "ℓ^a-rank". If in special circumstances we could insure

the G^v are cyclic, the correction factors due to ramification would vanish. At the expense of having larger correction factors we could prove a similar result over other base fields. We explore some of those variants in Section 3.

The referee pointed out that when ℓ is odd the lower bound in Proposition 2 can be improved to $t(t-3)/2$. We will not need this for our applications but since it is a significant improvement of our result we will present the argument in the appendix.

Section 2: The main theorems

We begin by assuming ℓ is an odd prime.

THEOREM 1: *Suppose that either $\ell^2 \nmid m$ and m is divisible by t primes congruent to 1 modulo ℓ, or $\ell^2 | m$ and m is divisible by $t-1$ primes congruent to 1 modulo ℓ. Let C_m^+ denote the class group of K_m^+. Then $r_\ell C_m^+ \geqslant t(t-3)/2$. In particular, if $t \geqslant 4$, $r_\ell C_m^+ \geqslant 2$, and $\ell^2 | h_m^+$.*

PROOF: Let L be the maximal ℓ-extension of $\mathbb{Q}$ in K_m^+. It is easy to see that the ℓ-rank of $G(L/\mathbb{Q})$ is t. Moreover, exactly t primes in $\mathbb{Q}$ ramify in L. By Proposition 2 we conclude $r_\ell C_L \geqslant [t(t-1)/2] - t = t(t-3)/2$. Finally, since K_m^+/L has degree prime of ℓ, the natural map from the ℓ-primary subgroup of C_L to C_m^+ is an injection, and we're done.

Theorem B of the introduction is, of course, a weak version of Theorem 1. We now take up the case $\ell = 2$. The ideas are the same as when ℓ is odd, but as usual the details are a bit more complicated.

Let L be the maximal 2-extension of $\mathbb{Q}$ in K_m and $L^+ = L \cap K_m^+$, the maximal 2-extension of $\mathbb{Q}$ in K_m^+. Define e^+ to be 1 if $-1 \in \mathbb{Q}$ is a local norm everywhere from L^+ but not a global norm, and to be 0 otherwise (see Proposition 2).

LEMMA 1: $e^+ = 0$.

PROOF; If m is a prime power $G(L^+/\mathbb{Q})$ is cyclic and the result follows from Hasse's norm theorem.

Suppose m is not a prime power and let p be an odd prime dividing m. We claim -1 is not a local norm at p from L^+. Suppose the contrary. Then -1 is a local norm at p from K_m^+ since $[K_m^+ : L^+]$ is odd. Since $[K_m : K_m^+]$ is unramified at all finite primes (in particular at p) it follows that -1 is a local norm at p from K_m and thus also from $K_p \subset K_m$. Suppose $u \in \mathbb{Q}_p(\zeta_p)$ with $Nu = -1$ (here N is the norm from $\mathbb{Q}_p(\zeta_p)$ to $\mathbb{Q}_p$). u is a local unit so there is a rational integer m such that $u \equiv m(1-\zeta_p)$. Hence $Nu \equiv m^{p-1} \equiv 1(1-\zeta_p)$. It follows that $-1 \equiv 1(1-\zeta_p)$ a contradiction.

We remark that when m is not a prime power and $2|m$ then -1 is also not a local norm at 2. The argument is the same except one uses the fact that $\zeta_4 \in K_m$ to derive a contradiction.

LEMMA 2: *If* $4/\varphi(m)$ *every prime ramified in* K_m *is ramified in* L^+.

PROOF: When $m = p^a$ is a prime power the result is immediate since p is totally ramified in K_m.

Assume m is not a prime power. Then K_m/K_m^+ is unramified at all finite primes. Also $[K_m^+ : L^+]$ is odd. Since every prime ramified in K_m has even ramification index, it follows that every prime ramified in K_m is ramified in L^+.

THEOREM 2: *Let* t *denote the number of odd primes dividing* m.

(i) Suppose m *is odd and divisible only by primes congruent to 1 modulo 4. Then* $r_2C_m^+ \geqslant t(t-3)/2$.

(ii) Suppose m *is odd and divisible by at least one prime congruent to 3 modulo 4. Then* $r_2C_m^+ \geqslant (t^2-5t+2)/2$.

(iii) Suppose $m = 4m_0$ *with* m_0 *odd. Then* $r_2C_m^+ \geqslant [t(-3)/2] - 1$.

(iv) Suppose $m = 2^a m_0$ *with* m_0 *odd and* $a \geqslant 3$. *Then* $r_2C_m^+ \geqslant [t(t-1)/2] - 3$.

PROOF: Recall that L^+ is the maximal 2-extension of $\mathbb{Q}$ in K_m^+. It suffices to find lower bounds for the 2-rank of the class group of L^+. For this we use Proposition 2 of Section 1 and Lemmas 1 and 2 above.

In case i) we have $r_2G(L^+/\mathbb{Q}) = t$ and t primes ramify. Thus $r_2C_{L^+} \geqslant [t(t-1)/2] - t = t(t-3)/2$.

In case (ii) let $p|m$ with $p \equiv 3(4)$. Then L is the composition of L^+ with $\mathbb{Q}(\sqrt{-p})$. It follows that $r_2G(L^+/\mathbb{Q}) = t-1$. Also t primes ramify. Thus

$$r_2C_{L^+} \geqslant [(t-1)(t-2)/2] - t = (t^2-5t+2)/2.$$

In case (iii) L is the compositum of L^+ with $\mathbb{Q}(\sqrt{-1})$. It follows that $r_2G(L^+/\mathbb{Q}) = t$. In this case $t+1$ primes ramify. Thus $r_2C_{L^+} \geqslant [t(t-1)/2] - (t+1) = [(t(t-3)/2] - 1$.

Case (iv) is slightly more complicated. Clearly $r_2G(L/\mathbb{Q}) = t+2$. Since L is the compositum of L^+ with $Q(\sqrt{-1})$ we have $r_2G(L^+/\mathbb{Q}) = t+1$. Moreover $t+1$ primes ramify in L^+. However, Proposition 2 is not directly applicable since the ramification group of 2 in L^+ may have rank 2. This will happen if m_0 is divisible by a prime $p \equiv 3(4)$ since then $L = L^+(\sqrt{-1}) = L^+(\sqrt{-p})$ which implies L/L^+ is unramified at all finite primes. Let G^v be the decomposition group of 2 in L^+. Then, $r_2G^v \leqslant 3$ and it follows that $H^2(G^v, \mathbb{Q}/\mathbb{Z})$ has 2-rank less than or equal

to 3. The method of proof of Proposition 2 shows $r_2C_{L^+} \geqslant [(t+1)t/2] - t - 3 = [t(t-1)/2] - 3$.

COROLLARY: *If m is odd and divisible exactly by four primes all congruent to 1 modulo 4 then $r_2C_m^+ \geqslant 2$.*

PROOF: This follows from case (i) of the theorem.

It is interesting to compare the results of Theorem 2 with those of Cornell given in [1]. Let's assume m is odd. Then we have shown $r_2C_m^+ \geqslant (t^2 - 5t + 2)/2$ which is positive for $t \geqslant 5$. In [1] Cornell shows $r_2C_m^+ \geqslant 2^{t-5} - 2$ which is positive for $t \geqslant 7$. Moreover, the lower bound given here is better for $t \leqslant 9$. For larger t our bound becomes rapidly inferior. The results of Kubert [8] concern the 2-divisibility of h_m^+ and are valid for $t \geqslant 7$. In this range he shows $2^a | h_m^+$ where $a = 2^{t-2} - [t(t-1)/2] - 2$.

Section 3: The case of two or three primes

As mentioned previously, we can prove some results by the methods of Proposition 2 even when m is only divisible by two or three primes. Instead of working with the maximal ℓ-extension of $\mathbb{Q}$ in K_m it is sometimes more convenient to work with smaller fields. The following lemma is very useful.

LEMMA: *Let $F/\mathbb{Q}$ be an abelian number field with group G. Suppose $G = T_1T_2 \ldots T_t$ is the direct product of all the finite inertia groups T_i. Then F has no proper unramified extension fields which are abelian over $\mathbb{Q}$.*

PROOF: Suppose E/F is unramified and $E/\mathbb{Q}$ is abelian. Let $T_1', T_2', \ldots, T_t'$ be the finite inertia groups for $E/\mathbb{Q}$. Since $\mathbb{Q}$ has no extensions ramified only at infinity, $G(E/\mathbb{Q}) = T_1'T_2' \ldots T_t'$. Since E/F is unramified $|T_i'| = |T_i|$ for each i. It follows that $|G(E/\mathbb{Q}| \leqslant |G(F/\mathbb{Q})|$ and so $E = F$.

COROLLARY: *Suppose $\mathbb{Q} \subset F \subset K_m^+$ and that F satisfies the hypothesis of the lemma. Then, the norm maps C_m^+ onto C_F.*

PROOF: Let H be the Hilbert class field of F. Then $H \cap K_m^+$ is an abelian extension of Q unramified over F. Thus $H \cap K_m^+ = F$ and so $G(K_m^+H/k_m^+) \approx G(H/F)$. The result follows.

Suppose ℓ is an odd prime and p_1, p_2 and p_3 are primes congruent to 1 modulo ℓ. Let F_i be the unique subfield of K_{p_i} which is of degree ℓ over Q, and $F = F_1F_2F_3$. Then, $F \subset K_{p_1p_2p_3}^+$, $G(F/\mathbb{Q}) \approx (\mathbb{Z}/\ell\mathbb{Z})^3$ and $G(F/\mathbb{Q}) = T_1T_2T_3$ where T_i is the inertia group of p_i in F. Finally, let G_i denote the decomposition group of p_i in F.

PROPOSITION 3: *Assume* $p_i \equiv 1(\ell)$ *for* $i = 1, 2, 3$. *In the following two situations we have* $\ell | h^+_{p_1p_2p_3}$.

(a) *The congruences* $x^\ell \equiv p_1(p_3)$ *and* $x^\ell \equiv p_2(p_3)$ *are solvable.*

(b) *The congruences* $x^\ell \equiv p_3(p_1)$ *and* $x^\ell \equiv p_3(p_2)$ *are solvable.*

PROOF: In case (a) the hypotheses imply that p_1 and p_2 split in F_3. Thus $G_1, G_2 \subseteq G(F/F_3)$. It follows that the image of both $H^{-3}(G_1, \mathbb{Z})$ and $H^{-3}(G_2, \mathbb{Z})$ in $H^{-3}(G(F/\mathbb{Q}), \mathbb{Z})$ lie in the image of $H^{-3}(G(F/F_3), \mathbb{Z})$. This latter group is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. Thus, the ℓ-rank of $\sum_{i=1}^3$ cor $H^{-3}(G_i, \mathbb{Z})$ is at most 2, whereas, the ℓ-rank of $H^{-3}(G(F/\mathbb{Q}), \mathbb{Z})$ is 3. The result now follows from the corollary to the Lemma.

In case (b) the hypothesis imply that p_3 splits in F_1 and F_2. Since p_3 ramifies totally in F_3 we see $G_3 = T_3$ which is cyclic. Thus $H^{-3}(G_3, \mathbb{Z})$ is trivial and the result follows as in case a).

PROPOSITION 4: *Let* ℓ *be an odd prime and* $p_1, p_2 \equiv 1(\ell)$ *primes. Suppose* $x^\ell \equiv p_1(p_2)$ *and* $x^\ell \equiv p_2(p_1)$ *are both solvable. Then* $\ell | h^+_{p_1p_2}$.

PROOF: Let F_1 and F_2 be the fields described above and $F = F_1F_2$. Then $F \subseteq K^+_{p_1p_2}$ and using the corollary to the Lemma it suffices to show $\ell \| C_F|$.

The hypothesis implies p_1 splits in F_2 and p_2 splits in F_1. It follows that $G_i = T_i$ for $i = 1, 2$ and so $H^{-3}(G_i, \mathbb{Z}) = (0)$ for $i = 1, 2$. Since $G(F/\mathbb{Q}) \approx (\mathbb{Z}/\ell\mathbb{Z})^2$, we have $H^{-3}(G(F/\mathbb{Q}), \mathbb{Z}) \approx \mathbb{Z}/\ell\mathbb{Z}$ and the result follows.

It should be remarked that there are infinitely many pairs of primes p_1 and p_2 satisfying the hypotheses of Proposition 4. To see this choose $p_1 \equiv 1(\ell)$ and let p_2 be a prime which splits completely in the field $Q(\zeta_\ell, \zeta_{p_1}, \sqrt[\ell]{p_1})$. Then $p_2 \equiv 1(\ell)$, $p_2 \equiv 1(p_1)$ and $x^\ell \equiv p_1(p_2)$ is solvable in $\mathbb{Z}$. So is $x^\ell \equiv p_2(p_1)$ since $p_2 \equiv 1(p_1)$. Thus p_1 and p_2 are a pair of the required type.

We conclude with two results about the situation when $\ell = 2$.

PROPOSITION 5: *Suppose* p_1, p_2 *and* p_3 *are primes congruent to* 1 *modulo* 4. *Suppose* $x^2 \equiv p_1(p_3)$ *and* $x^2 \equiv p_2(p_3)$ *are both solvable. Then* $2 | h^+_{p_1p_2p_3}$.

PROOF: Let $F_i = \mathbb{Q}(\sqrt{p_i})$ for $i = 1, 2, 3$ and $F = F_1F_2F_3$. Then $F \subset K^+_{p_1p_2p_3}$ and $G(F/\mathbb{Q}) \approx (\mathbb{Z}/2\mathbb{Z})^3$. The hypothesis implies that p_1 and p_2 split in F_3 and so $G_1, G_2 \subseteq G(F/F_3)$. By quadratic reciprocity, $x^2 \equiv p_3(p_1)$ and $x^2 \equiv p_3(p_2)$ are both solvable so that p_3 splits in both F_1 and F_2. Thus $G_3 = T_3$ and is cyclic. From these remarks and the proof of Proposition 3, we see $\sum_{i=1}^3$ cor $H^{-3}(G_i, \mathbb{Z}) \subset H^{-3}(G(G/\mathbb{Q}), \mathbb{Z})$ is of 2-rank at most 1, whereas, $r_2 H^{-3}(G(F/\mathbb{Q}), \mathbb{Z}) = 3$. Thus $r_2 A(F/\mathbb{Q}) \geqslant 2$ whereas $r_2 B(F/\mathbb{Q}) \leqslant 1$. It follows from Proposition 1 that $2 | h_F$, and by the corollary to the Lemma, $2 | h^+_{p_1p_2p_3}$.

PROPOSITION 6: *Suppose p_1 and p_2 are primes congruent to* 1 *modulo* 8, *and that $x^4 \equiv p_1(p_2)$ and $x^4 \equiv p_2(p_1)$ are both solvable. Then $2 | h^+_{p_1 p_2}$.*

PROOF: Let F_i denote the real cyclic extension of $\mathbb{Q}$ contained in K_{p_i} such that $[F_i : \mathbb{Q}] = 4$ for $i = 1, 2$. Let $F = F_1 F_2$. Then $F \subset K^+_{p_1 p_2}$ and $G(F/\mathbb{Q}) \approx (\mathbb{Z}/4\mathbb{Z})^2$. The hypothesis implies p_1 splits in F_2 and p_2 splits in F_1. Thus $G_i = T_i$ for $i = 1, 2$ and are thus cyclic. Consequently, $H^{-3}(G(F/\mathbb{Q}), \mathbb{Z}) \approx \mathbb{Z}/4\mathbb{Z}$ whereas $H^{-3}(G_i, \mathbb{Z}) = (0)$ for $i = 1, 2$. From this we deduce $|A(L/K)| = 4$ whereas $|B(L/K)| \leqslant 2$. By Proposition 1, $2 | h_F$, and invoking the corollary to the Lemma once again, $2 | h^+_{p_1 p_2}$.

We note the same ideas can be used to show the following. Let $p_1 \equiv 1(4)$, $p_2 \equiv 3(4)$, and suppose $x^2 \equiv p_1(p_2)$ and $x^2 \equiv p_2(p_1)$ are both solvable. Then $2 | h_{p_1 p_2}$. This is made possible by the fact that -1 is not a local norm at infinity from the field $Q(\sqrt{p_1}, \sqrt{-p_2})$. For example, 2 divides h_{39} and h_{95}. On the other hand $h^+_{39} = h^+_{95} = 1$.

Appendix

We would like to thank the referee for the following proposition and its proof.

PROPOSITION 7: *Let ℓ be an odd prime and $L/\mathbb{Q}$ an abelian ℓ-extension with $r_\ell G(L/\mathbb{Q}) = t$. Then $r_\ell C_L \geqslant (t(t-3))/2$.*

Before giving the proof we state and prove a group-theoretical lemma which will be needed.

LEMMA: *Let ℓ be an odd prime, Γ a finite ℓ-group with commutator subgroup contained in its center. Then $a^\ell = e = b^\ell$ implies $(ab)^\ell = e$.*

PROOF: Set $c = a^{-1}b^{-1}ab$. Then, by induction on i we find $a^i b = b a^i c^i$. Setting $i = \ell$ we find $c^\ell = e$. Using induction one again we find $a^i b^i = (ab)^i c^{i(i-1)/2}$. Setting $i = \ell$ in this relation yields the result.

PROOF OF PROPOSITION 7: Assume to begin with that $G(L/\mathbb{Q})$ is an elementary abelian ℓ-group. Let L_g and L_c denote the genus and central class field of $L/\mathbb{Q}$. By a result of Furuta [4] we know $G(L_c/L_g) \approx A(L/\mathbb{Q})/B(L/\mathbb{Q})$. By Proposition 2 it follows that $r_\ell G(L_c/L_g) \geqslant [t(t-1)/2] - s$. Using the genus formula of Leopoldt [10] we find $r_\ell G(L_g/L) = s - t$). If we can show $G(L_c/L)$ is an elementary abelian ℓ-group then $r_\ell G(L_c/L) \geqslant [t(t-1)/2] - s + s - t = t(t-3)/2$ which gives the result in this case. Let $\Gamma = G(L_c/Q)$. The commutator subgroup of Γ is contained in its center. Moreover Γ is generated by its inertia subgroups and these are cyclic of order ℓ. It follows from the Lemma that every

element of Γ has order ℓ and so $G(L_c/L) \subset \Gamma$ is an elementary abelian ℓ-group as required.

Suppose now that $G(L/\mathbb{Q})$ is an abelian ℓ-group and let L' be the maximal elementary abelian ℓ-extension of Q contained in L. Let H' be the Hilbert class field of L'. Applying the above argument to L' one sees that it suffices to check what $L \cap H' = L'$. Now, $L \cap H'$ is an abelian extension of Q which is unramified over L'. Thus, it is contained in the genus field of L' and it follows that $G(L \cap H'/\mathbb{Q})$ is an elementary abelian ℓ-group. By the maximality of L' we have $L \cap H' = L'$ and the proof is complete.

References

[1] G. CORNELL: Exponential growth of the ℓ-rank of the class group of the maximal real subfield of cyclotomic fields (to appear).

[2] A. FRÖHLICH: On the absolute class group of abelian fields, *J. of the London Math. Soc. 29* (1954) 211–217.

[3] A. FRÖHLICH: On the absolute class group of abelian fields II, *J. of the London Math. Soc. 30* (1955) 72–80.

[4] Y. FURUTA: On class field towers and the rank of ideal class groups, *Nagoya Math. J. 48* (1972) 147–157.

[5] D. GARBANATI: Ivariants of the ideal class group and the Hasse norm theorem, *J. Reine and Angew. Math. 297* (1978) 159–171.

[6] F. GERTH: The Hasse Norm theorem for abelian extensions of number fields, *Bulletin Amer. Math. Soc. 83* (1977) 264–266.

[7] B. HUPPERT: *Endliche Gruppen I.* Berlin Heidelberg, New York: Springer-Verlag (1979).

[8] D. KUBERT: The 2-divisibility of the class number of cyclotomic fields and the Stickelberger ideal (to appear).

[9] S. LANG: Units and class groups in number theory and algebraic geometry, *Bullentin Amer. Math. Soc. 6* (1982) 253–316.

[10] H.W. LEOPOLDT: Zur Geschlechtertheorie in abelschen Zahlkörpern, *Math. Nach. 9* (1953) 350–362.

[11] M. RAZAR: Central and genus class fields and the Hasse norm theorem, *Comp. Math. 35* (1977) 281–298.

[12] K. YAMAZAKI: On projective representations and ring extensions of finite groups, *J. Fac. Sci. Univ. Tokyo 10* (1964) 147–195.

(Oblatum 23-VI-1982, 19-X-1982 & 27-I-1983)

Gary Cornell
Department of Mathematics
University of Connecticut
Storrs, CT 06268
USA

Michael I. Rosen
Department of Mathematics
Brown University
Providence, RI 02912
USA