RESEARCH ANNOUNCEMENTS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 8, Number 1, January 1983

EXPONENTIAL GROWTH OF THE l-RANK OF THE CLASS GROUP OF THE MAXIMAL REAL SUBFIELD OF CYCLOTOMIC FIELDS

GARY CORNELL

Introduction. Let K_m be the mth cyclotomic field, so $K_m = Q(e^{2\pi i/m})$ with m not congruent to 2 modulo 4. The maximal real subfield of K_m, K_m^+ and its class number h_m^+ (sometimes called the real class number and sometimes the second factor) is of interest not only to number theorists but to mathematicians in other fields as well. For example, the power of two dividing h_m^+ is tied to classifying certain actions of groups on spheres. (Lang's survey article [7] gives a number of references for this.) However, the real class number is difficult to compute and general information on its size has been hard to come by.

Class Field Theory says that to understand the class group of a number field it would be enough to construct all the unramified abelian extensions of it. A natural idea is to try to construct unramified abelian extensions of a large field by means of abelian (possibly ramified) extensions of some smaller field whose ramification 'collapses' when translated over to the larger field. This idea stems from two seminal papers of Fröhlich [4, 5] where he defined the (absolute) genus field as the largest unramified abelian extension of a number field obtained by composing it with an absolutely abelian field. Unfortunately, it is easy to see that such absolutely abelian translates will never give properly larger abelian unramified extensions of either a full cyclotomic field or its maximal real subfield. Recently [1, 3] it has been shown that by using a properly chosen subfield of a cyclotomic field and abelian extensions of that field (relative genus theory) information about cyclotomic class numbers can be obtained.

This note sketches results obtained by relative genus theory about the class number of cyclotomic fields. Among other results we show that, contrary to what some have believed, the real class number is often quite large. Kubert [6] had earlier obtained results by totally different methods that parallel some of the results obtained here.

Received by the editors May 26, 1982.
1980 *Mathematics Subject Classification.* Primary 12A35.

0273-0979/82/0000-1034/$01.50

The results. The first observation needed is that there are certain subfields E of K_m^+ whose Hilbert class fields, H_E, do not collapse when translated to any absolutely abelian extension. For example

LEMMA. *Let $E \subset K_m^+$ where $\mathrm{Gal}(E/Q)$ is the direct sum of its inertia groups; then for any absolutely abelian K, $H_E \cap K \subset E$.*

PROOF. This is an obvious consequence of the fact that Q has no unramified extensions.

Next, for any odd prime l the maximal elementary abelian l-extension of Q contained in K_m^+ is a field, E, of the type considered in the lemma above. The rank of $\mathrm{Gal}(E/Q)$ is $t+\epsilon$ where t is the number of primes congruent to 1 modulo l dividing m and $\epsilon = 1$ if l^2 divides m and 0 otherwise. We will apply relative genus theory to E. We need a technical lemma (due to Abhyankar).

ABHYANKAR'S LEMMA. *Suppose E_1, E_2 are abelian extensions of some field F. Assume E_2/F is tamely ramified and the ramification index of every prime ramified in E_2 divides the ramification of the corresponding prime in E_1, then E_1E_2/E_1 is unramified.*

(For a proof see [1].)

We want to show that E has a large relative genus field with respect to some properly chosen subfield. Suppose $t+\epsilon > 4$ and choose p, q dividing m, $p \equiv q \equiv 1(l)$. Let F_1 be the decomposition field for p and F_2 the decomposition field for q in E. Both p and q split completely in $F = F_1 \cap F_2$. Moreover, F has degree at least $l^{t+\epsilon-4}$ over Q because inertia groups are cyclic for these real abelian fields and so the decomposition groups can have l-rank at most 2. Say $p = \mathcal{P}_1 \ldots \mathcal{P}_s$, $q = q_1 \ldots q_s$, $s = [F : Q]$. Let $\mathcal{A}$ be the integral ideal of F obtained by dividing pq by one of the primes above p and one of the primes above q. Let $F^{\mathcal{A}}$ be the full ray class field of F with modulus $\mathcal{A}$.

LEMMA. *$F^{\mathcal{A}}$ has a subfield K containing the Hilbert class field of F, H_F, such that $\mathrm{Gal}(K/H_F) \simeq (Z/l)^{s-1}$ and every prime of F to K has ramification index either 1 or l.*

PROOF. This follows from class field theory since

$$\mathrm{Gal}(F^{\mathcal{A}}/H_F) \simeq (\mathcal{O}/\mathcal{A})^*/u/u^1(\mathcal{A})$$

where $u/u^1(\mathcal{A})$ is the quotient group of the units by the units congruent to 1 modulo $\mathcal{A}$. The result now follows because all the inertia groups are cyclic and the l-rank of $(Z/\mathcal{A})^*$ is $2s-2$ while the l-rank of $U/U^1(\mathcal{A})$ can be at most $s-1$.

Notice that K satisfies the conditions of Abhyankar's lemma with respect to E, so KE/E is unramified. We want to show $G(KE/E)$ has large l-rank. It is enough to show $K \cap E \subset H_F$. This is easily seen because the only primes that could ramify are the ones dividing $\mathcal{A}$, while $K \cap E$ being absolutely abelian must have all the primes above $p(q)$ ramify if any did. Thus $E \cap K \subset H_F$ and we've shown

THEOREM. *The l-rank of the class group of E has rank $\geq l^{t+\epsilon-4} - 1$.*

But because of the first lemma we've also shown

THEOREM. *K_m^+ has l-class rank $\geq l^{t+\epsilon-4}-1$ and so $l^{l^{t+\epsilon-4}-1} \Big| h_m^+$.*

Since we've shown the l-rank is so large, it's natural to apply this result to class field towers, we have

THEOREM. *For $l > 5$ every cyclotomic field having more than 5 primes $\equiv 1\ (l)$ in the discriminant (or 4 if l^2 divides m) has an infinite l-class field tower.*

REMARKS. It's not hard to see that the choice of primes above p and q deleted make no difference in the field EK obtained. So no more information can be obtained that way. However, we've made no special assumptions about p and q (save that they were not l) and so the same game can be played for every pair. Complications set in because it must be shown that the various ray class fields involved are "sufficiently" disjoint. It is not hard to show that with the hypothesis above.

THEOREM. *There exists a constant $C > 1$ dependent on m such that the l-class rank of K_m^+ is $\geq C[l^{t+\epsilon-4}-1]$. (A reasonable conjecture is the constant is more or less $\binom{t}{2}$.)*

When $l = 2$ the same proof will work except for modifications caused by: The maximal real 2-subfield has a slightly more complicated structure and the existence of ± 1 must be taken into account. As an example of the kind of theorem possible we have

THEOREM. *The 2-rank of the class group of K_m^+ is $\geq 2^{t-5}-2$ where t is the number of odd primes dividing m.*

Various extensions are possible; see [2] for details.

Now a simple argument using the prime number theorem shows that the product of the first t primes is of order of magnitude t^t and so

THEOREM. *For any positive integer a there exist infinitely many m such that $h_m^+ > m^a$.*

ACKNOWLEDGEMENTS. This work was originally done for odd primes and aimed towards the connections with class field towers. It was only after reading about Kubert's results in the early version of [7] that I decided to extend these results to $l = 2$.

Finally, M. Rosen first suggested relative genus theory as a thesis topic and all my subsequent research has benefitted from his insights. The Vaughn Foundation generosity has also been most helpful.

BIBLIOGRAPHY

1. G. Cornell, *Abhyankar's lemma and the class group*, Number Theory (Carbondale), Lecture Notes in Math., vol. 751, Springer-Verlag, Berlin and New York, pp. 82–88.
2. ____, *Exponential growth of the l-rank of the class group in the maximal real subfield of cyclotomic fields and in related fields* (in preparation).

3. G. Cornell and L. Washington, *Class numbers of cyclotomic fields*, J. Number Theory (to appear).
4. A. Fröhlich, *Genus field and genus group in finite number fields.* I, Mathematica **6** (1959), 40–46.
5. ____, *Genus field and genus group in finite number fields.* II, Mathematica **6** (1959), 142–146.
6. D. Kubert, *The 2-primary part of the ideal class group of cyclotomic fields* (to appear).
7. S. Lang, *Units and class groups in number theory and algebraic geometry*, Bull. Amer. Math. Soc. (N.S.) **6** (1982), 253–316.

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