数理解析研究所講究録
第 603 巻 1987 年 93-101

The Structure of the Ray Class Group

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

Introduction: Suppose you are given a number field **K**; for whichprimes $\mathfrak{p}$ is there a cyclic extension of K of degree n totally and only ramified at $\mathfrak{p}$? When **K** = $\mathbb{Q}$ the answer is well known: for it follows from the Kronecker-Weber theorem that any such extension in contained in $\mathbb{Q}(\zeta_{p}a)$ for some a>0 and therefore such an extension exists if and only if there is a cyclic quotient group of $(\mathbb{Z}/p^{a})^{*}$ of order n. In general, if **K** contains the n'th roots of unity then much can be said here also. If, however, **K** does not contain the n^{th} roots of unity then little seems to be known. This paper is an exposition of work that is still in progress on this problem.

Continuing the analogy with cyclotomic fields: we know by class field theory that any such extension would be contained in the ray class field with conductor $\mathfrak{p}^{a}$ for some a > 0. We will denote the ray class field with conductor $\mathfrak{a}$ by $K(\mathfrak{a})$. In fact if we restrict ourselves to the case when $(n, \mathfrak{p}) = 1$ we know a would have to be one. (Any tamely ramified extension has a square-free conductor). However here complications set in because the group $K(\mathfrak{a})$ contains the Hilbert Class field of K, H_K and the tower of fields $K \subset H_K \subset K(\mathfrak{a})$ corresponds to a short exact sequence of groups:

$$\frac{(\mathcal{O}/\mathfrak{a})^*}{U/U^1(\mathfrak{a})} \dashrightarrow I_{\mathfrak{a}}/_{P_{\mathfrak{a}}} \dashrightarrow C_K$$

where $\mathcal{O}$ is the ring of integers in K, U (resp. $U^1(\mathfrak{a})$) is the unit group (units $\equiv 1\ (\mathfrak{a})$). $I_{\mathfrak{a}}$ is the group generated by ideals prime to $\mathfrak{a}$, $P_{\mathfrak{a}}$ is the set of principal ideals containing a generator congruent (multiplicatively) to 1 (mod $\mathfrak{a}$) and finally C_K is the class group. If $\mathfrak{a}$ were a power of a prime ideal $\mathfrak{p}$ then the group is the inertia group $T(\mathfrak{p})$ in this extension. (See Lang for a proof of this or any of the other facts from class field theory we may need.) Thus our problem reduces to showing:

1) n divides the order of $\dfrac{(\mathcal{O}/\mathfrak{a})^*}{U/U^1(\mathfrak{a})}$

2) There exists a subgroup of *index* n not containing $T(\mathfrak{p})$.

Note that if n doesn't divide the class number of K, h_K then of course the exact sequence * splits at n and 1) is both necessary and sufficient. If n divides h_K then as we shall see it is quite possible that the first condition is satisfied but the second is not.

The author would like to thank Profs. M. Isaacs, H. W Lenstra Jr. and M. Rosen for many helpful discussions. Finally, there remains only the pleasant task of thanking the Taniguchi foundation and my many colleagues in Japan that made this trip so valuable.

First off we show there exists a set of primes of positive density for which n divides $|\mathbb{T}(\mathfrak{p})|$.

Theorem 1: Let n and a finite extension K/Q be given. Then there exists a finite extension L of K with the property that every prime ideal that is above a prime ideal that splits completely from Q to L satisfies $n \mid |\mathbb{T}(\mathfrak{p})|$.

We need to show that the index of the group $U/U^1(\mathfrak{p})$ in $(\mathcal{O}/\mathfrak{p})^*$ is divisible by n. Let $L = K(U^{1/n})$ where U is the unit group of K. This contains ζ_n and is a finite extension of Q by the Dirichlet unit theorem. We claim any prime of Q that splits completely in L satisfies the conditions of the theorem. To prove this note that when a prime splits completely in L, the completion at any of the primes above p is just $\mathbb{Q}_p$. Moreover every global unit is locally an n'th power since the polynomial $X^n - u$ splits completely in $\mathbb{Q}_p$. Now $(\mathcal{O}/\mathfrak{p})^*$ is isomorphic to the completion of $\mathcal{O}$ modulo the completion of $\mathfrak{p}$ and so we have the global units map entirely into the n'th powers of the local units. But, given any finite abelian group Γ with $n \,/\, |\Gamma|$ the index of Γ^n in Γ is a multiple of n. Since we have chosen p to split completely in a field containing the n'th roots of unity, we also have $N\mathfrak{p} = p \equiv 1$ (ℓ). The theorem now follows.

Remark: It's not hard to see that for $(\ell,n)=1$, $\alpha \equiv 1 \pmod{\ell}$ implies that α is locally an n'th power. For this reason the above condition on K is more or less forced. It is also possible to strengthen this theorem somewhat if $\zeta_p \not\in K$. One can then prove:

Theorem: There exists a set of primes of positive density such than n divides $|T_{\mathfrak{p}}|$ but pn does not.

In any case we have now answered our question for the case when n and the class number of K are relatively prime. For any prime with n dividing $|T_{\mathfrak{p}}|$ will serve. We now turn to the more general situation and we first show that the problem can be solved when the field K contains the n'th roots of unity. For that we need some standard results from Kummer theory.

lemma 1: For any field K containing the n'th roots of unity and $\alpha \varepsilon K$; the extension $K(\sqrt[n]{\alpha})$ can be ramified only at the primes dividing (α) and the primes dividing n.

Another standard results allows us to eliminate the possibility that any primes dividing n ramify.

lemma 2: Suppose K contains the n'th roots of unity, α is in L and α is an n'th power residue modulo a sufficiently high power at all the primes dividing n. Then $K(\sqrt[n]{a})$ can only be ramified at the prime ideal dividing (α).

Finally we need to insure that the primes dividing (α) *do ramify.*

lemma 3: If (α) is not divisible by the n'th power of any ideal then all the primes dividing (α) *do* ramify in $K(\sqrt[n]{\alpha})$.

All these are standard facts from local Kummer theory.
Now to:

Theorem 2: Suppose K contains the n'th roots of unity then there exists a set of primes of positive density so that for each prime $\mathfrak{p}$ in this set there exists a cyclic extension of K of degree n ramified only and totally at $\mathfrak{p}$.

proof: Let L be the full ray class field of K with conductor n^b and let $\mathfrak{p}$ be any prime from K that splits completely in this field. By class field theory this can happen if and only if $\mathfrak{p}$ is a principal prime (π) which is also congruent multiplicatively to 1 modulo n^b. By the previous lemmas $K(\sqrt[n]{\pi})$ satisfies the conditions of the theorem.

Remarks:. It would be interesting to know the minimal conditions for such primes to exist in Kummer extensions.

We now want to sketch a proof of our main theorem which roughly says that if you want to solve the problem for a field K, it's enough to solve it for $K(\zeta_n)$.

Theorem 4: Suppose a prime $\mathfrak{p}$ is given with $N(\mathfrak{p}) \equiv 1$ (n). Suppose for each $\mathcal{P}$ above $\mathfrak{p}$ in $K(\zeta_n)$ there exists a cyclic extension of degree n totally (and only) ramified at $\mathcal{P}$. Then K has a cyclic extension of degree n totally (and only) ramified at $\mathfrak{p}$.

Remarks: Since $Gal(K(\zeta_n)/K) = \Delta$ acts transitively on the primes above $\mathfrak{p}$ its enough to have such an extension at one of the primes above $\mathfrak{p}$. For then the extension of $K(\zeta_n)$ which is ramified at $\mathcal{P}$ say, can be mapped by an element of $Gal(K(\zeta_n)/K)$ to one ramified at $\mathcal{P}'$. Essentially then what we need to do is relate the structure of the ray class field L of $K(\zeta_n)$ with conductor $\mathfrak{p}$, when $\mathfrak{p}$ is considered as an integral ideal in $K(\zeta_n)$ to the ray class field of K with conductor $\mathfrak{p}$.

lemma: Let F be the composite of all the individual cyclic extension of degree n ramified at the primes $\mathcal{P}$ above $\mathfrak{p}$. This is a galois extension of K. Moreover this galois group is a split extension of a group of type $(\mathbb{Z}/n)^d$ where d is the degree $[K(\zeta_n):K]$ and a cyclic group of order d.

proof:The extension F/K is a galois extension because we have taken *all* the cyclic extensions of degree n ramified at the primes $\mathcal{P}$ above $\mathfrak{p}$. It is, in fact, the maximal abelian extension of $K(\zeta_n)$ of exponent n ramified at the primes above $\mathfrak{p}$. If we let T_i be the ramification group of $\mathcal{P}_i$ then $gal(K(\zeta_n)/K)$ acts transitively on each of these cyclic extensions and so permutes the $T_i \cong \mathbb{Z}/n$. This in turn implies that $T_1 \ldots T_d = gal(F/K(\zeta_n)$ is a free $Z/n[\Delta]$ module.

Such a module has trivial cohomology in all dimensions and therefore the extension splits.

Remark: these types of groups occur often and are called wreath products. This group contains a normal subgroup isomorphic to $(\mathbb{Z}/n)^d$ and also a non-normal cyclic subgroup of order d disjoint from the $(\mathbb{Z}/n)^d$.

Claim: The commutator subgroup of the galois group of F over K is isomorphic to $(\mathbb{Z}/n)^{d-1}$ and is disjoint from the inertia groups of any of the primes above $\mathfrak{p}$.

Suppose we accept the claim, then the proof can be finished as follows: Let **H** be the normal subgroup of Gal(F/K) of index n which is obtained by taking the commutator subgroup together with the non-normal subgroup of order d described above. The fixed field of this group is a cyclic extension of K of degree n ramified only (and totally) at $\mathfrak{p}$.

So what remains is to prove the claim about the commutator subgroup. We can actually prove a bit more. (Although this is probably well known I was unable to find a reference so I include a short, computational proof)>

Theorem: The commutator subgroup of gal(F/K) is the set of elements $x_1^{a_1}x_2^{a_2}\ldots x_d^{a_d}$ in $T_i \ldots T_d$ where $\Sigma a_i \equiv 0$ (n).

We need a way of describing this group so that we can compute the commutators. We will let $\langle\alpha\rangle$ be the cyclic group of order d that acts on the various subgroups T_i of type $\mathbb{Z}/n$. We denote the elements in T_i by x_i, y_i etc. The group can then be completely defined by specifying that α^s sends x_i to x_{i+s}, i.e. that $\alpha^s T_i \alpha^{-s} = T_s$ (where i+s is read modulo d). Consider the commutator $[\alpha^s, t_i] = \alpha^s t_i \alpha^{-s} t_i^{-1} = t_s t_1^{-1}$. This proves our claim for simple commutators.For the general case just expand the general commutator $[\alpha^s x_i y_j \ldots z_k, \alpha^t b_i \ldots c_k]$

Remark: Notice that this gives us an independent proof of the remark before theorem 1.

Finally, non-existence is a much more subtle problem. For example consider the naive approach to non-existence through the following theorem:

Theorem Let K be a number field containing the n'th roots of unity with a non-trivial ℓ-class group. Let $\mathfrak{p}$ a prime ideal such that $[\mathfrak{p}]$ has maximal ℓ order in a direct summand of the class group of K; then K can have no extension of degree ℓ ramified only at $\mathfrak{p}$.

proof: Suppose such an extension F exists then there exists an element α in K such that $F(\sqrt[\ell]{\alpha})$ yields a cyclic extension of K ramified only at $\mathfrak{p}$. This means that $(\alpha) = \mathfrak{p}^e \mathfrak{a}^\ell$. But

$\mathfrak{p}^{e(e,\ell)} = 1$ also has maximal ℓ order in a summand of the class group so it times an ℓ'th power can never be principal.

The problems with using this naive approach arise because we must ask the question: To what extent does the hypothesis "having maximal ℓ-order in a summand of the class group" not contradict the hypothesis "splitting completely in $K(\sqrt[\ell]{U})$"?. Notice however that this naive approach *will* work if K properly contains a field k with $k(\zeta_\ell) = K$ and k had a non-trivial ℓ-class group. (For then the ℓ-class group of k is a direct summand of the ℓ class group of $k(\zeta_\ell) = K$).

Since this work is still in progress we must leave a fuller treatment of these questions to another paper.

BIBLIOGRAPHY

Lang, S. Algebraic Number Theory, reprint Springer Verlag 1986.