A REMARK ON CLASS NUMBERS OF NUMBER FIELD EXTENSIONS[1]

JOHN SMITH

In this note we study some cases in which the structure of the Galois group of an extension of number fields gives information about the relation between the ideal class groups of these fields. The letters K, L, etc. will denote finite extension fields of the rationals and the letter p will denote a rational prime. If A is an abelian group we let its order be denoted by $|A|$ and its p-sylow subgroup by A_p. The class group of L will be written Cl_L.

LEMMA 1. *Let S be a set of automorphisms of L, satisfying $\sigma \neq 1$, $\sigma^2 = 1$, for all $\sigma \in S$. Let H be the group of products of even numbers of elements of S. Then if p does not divide the class number of the fixed field of any of the $\sigma \in S$, the action of H on $(\mathrm{Cl}_L)_p$ is trivial.*

PROOF. It will suffice to show that $(C)^\sigma = C^{-1}$, $\sigma \in S$, $C \in (\mathrm{Cl}_L)_p$. Let I be an ideal of L representing C. Then for some n, $I^{p^n} = (a)$, the principal ideal generated by $a \in L$. Now $II^\sigma = J$, the extension to L of an ideal of the fixed field of σ. Hence $J^{p^n} = (aa^\sigma)^{p^n} = (b)$, b in the fixed field of σ. But from our assumption on the class number of this field it follows that $J = (c)$, c in L, hence $CC^\sigma = 1$.

COROLLARY. *Let L, S, H, p be as above, let M be the maximum unramified abelian p-extension of L, and let K be the fixed field of H. Then $G(M/L) \subset Z(G(M/K))$ (the center).*

THEOREM 1. *Let S be a set of automorphisms of order 2 of L and K the fixed field of the group, H, of products of even numbers of elements of S. Then for any p, prime to the order of H and to the class number of the fixed field of each $\sigma \in S$, the p-Sylow subgroups of the class groups of L and K are isomorphic.*

PROOF. Let M be as in the Corollary. Then since $[M:L]$ is prime to $[L:K]$ the sequence $\{1\} \to G(M/L) \to G(M/K) \to G(L/K) \to \{1\}$ splits and since $G(M/L) \subset Z(G(M/K))$ the sum is direct. Therefore there is an N, $M \subset N \subset K$ with $NL = M$, $N \cap L = K$, $G(N/K)$

Presented to the Society, January 23, 1968 under the title *A remark on class groups of extensions with certain types of Galois groups;* received by the editors April 17, 1967 and, in revised form, October 9, 1967.

[1] Part of this work was supported by an NSF contract through the University of Michigan and was done at an NSF summer seminar at Bowdoin College.

$\cong G(M/L)$. N/K is unramified, for any ramified prime would have its ramification index from K to M divisible by p. Hence it is contained in the maximum unramified abelian p-extension, N', of K. But since $N' \subset M$, $N = N'$ and the theorem is proved.

COROLLARY 1. *Let $G(L/K)$ be a nonabelian simple group. Suppose p does not divide $[L:K]$ and does not divide the class number of the fixed field of some σ of order 2 in $G(L/K)$. Then $(\mathrm{Cl}_L)_p \cong (\mathrm{Cl}_K)_p$.*

PROOF. We take as our set S the conjugates of σ. This is a normal set, hence H is normal, hence equal to $G(L/K)$.

REMARK. The above may be rephrased by saying that for any p not dividing $[L:K]$ for which $(\mathrm{Cl}_L)_p \ncong (\mathrm{Cl}_K)_p$, p divides the class numbers of all subextensions of codegree 2. (We know there are such fields by the Feit-Thompson theorem.)

We now consider the case where $G(L/F)$ is dihedral. The following lemma will be useful.

LEMMA 2. *Let $G(L/K)$ be cyclic and suppose it acts trivially on $(\mathrm{Cl}_L)_p$. Suppose further that p^n divides the exponent of Cl_L but not that of $G(L/K)$. Then p divides $|\mathrm{Cl}_K|$.*

PROOF. Let M be the maximum unramified abelian p-extension of L. Then $G(M/L) \subset Z(G(M/K))$ and $G(L/K)$ is cyclic. Hence $G(M/K)$ is abelian. It contains an element of order p^n; hence there is a cyclic subextension N/K of degree p^n. No prime ramifies totally on N/K for then there would be an element of order p^n in an inertial group of $G(M/K)$, which is impossible. Hence the subextension of N/K of degree p is unramified, so p divides $|\mathrm{Cl}_K|$.

Now if $G(L/F)$ is dihedral of order $2m$, m odd, any 2 elements of order 2 are conjugate and the even products of such elements form the unique subgroup, H, of order m.

COROLLARY 2. *Let $G(L/F)$ be dihedral of order $2m$, m odd, E/F a subextension of degree m and K the unique quadratic subextension. Then if p^n divides the exponent of Cl_L $(n \geqq 1)$ but p does not divide $|\mathrm{Cl}_E|$ and p^n does not divde m, then p divides $|\mathrm{Cl}_K|$. If, in addition, $(p, m) = 1$, then $(\mathrm{Cl}_L)_p \cong (\mathrm{Cl}_K)_p$.*

PROOF. The first assertion follows from Lemmas 1 and 2, the second from Theorem 1.

COROLLARY 3. *Let $G(L/F) \cong S_n$, (the symmetric group), $n \neq 4$, and let K be the fixed field of the alternating group A_n. Then for any $p > n$, and any subextension E/F such that $[L:E] = 2$, either p divides $|\mathrm{Cl}_E|$ or $(\mathrm{Cl}_L)_p \cong (\mathrm{Cl}_K)_p$.*

PROOF. The result is trivial if $n=2$ and contained in Corollary 2 if $n=3$. For $n\geqq 5$, Corollary 1 applies if $E\supset K$; otherwise one must resort to Theorem 1 itself.

COROLLARY 4. *Let $G(L/K)$ be an abelian 2-group. Then any odd prime p dividing the class number of L divides the class number of some intermediate field E where E/K is cyclic.*

PROOF. Let E be an intermediate field whose class number is divisible by p and which is minimal with respect to this property. If E/K is not cyclic then there are subextensions F, F' and F'' of codegree two with $F\cap F'\subset F''$. If p does not divide the class numbers of F and F' then applying the theorem we have that the p-primary parts of the class groups of E and F'' are isomorphic.

REMARK. In the special case of a special biquadratic extension of the rationals a much stronger result is well known (see [1], p. 51).

REFERENCE

1. D. Hilbert, *Gesammelte Abhandlungen*, Vol. I, Chelsea, New York, 1965.

BOSTON COLLEGE