CLASS NUMBER AND RAMIFICATION IN NUMBER FIELDS

ARMAND BRUMER and MICHAEL ROSEN

1. Introduction. In the ring O_K of algebraic integers of a number field K, the group I_K of ideals of O_K modulo the subgroup P_K of principal ideals is a finite abelian group of order h_K, the class number of K. The determination of this number is an outstanding problem of algebraic number theory.

Leopold has shown in [1] that if K is an absolutely abelian extension of degree m over the rationals Q, and $e_1, e_2, \ldots, e_n$ are the ramification degrees of the ramified prime ideals of K, then $\Pi_{s=1}^{r} e_s/m$ divides h_K.

The aim of this paper is to prove the following partial generalization.

Main Theorem. *Let K be a number field of degree m over the rationals and L be a Galois extension of K of relative degree $[L : K] = n$. Then there is an integer $R(m, n)$ depending only on m and n such that $h_K \Pi_{s=1}^{r} e_s/R(m, n)$ divides h_L, where $e_1, e_2, \ldots, e_r$ are the ramification degrees of all the prime ideals of K which are ramified in L.*

This theorem has the following qualitative result as immediate consequence.

Corollary. *Let K be a number field and consider the set of Galois extensions L of K of relative degree n. Then the class number of L goes to infinity with the number of prime ideals of K which are ramified in L.*

The idea of the proof of our main result is to first give an arithmetic interpretation to the cohomology group $H^1(G, U_L)$ where L is a Galois extension of the number field K, G is the Galois group of the extension and U_L is the group of units of O_L. Then in section 3, we shall find a bound on $H^1(G, U_L)$ by using the Dirichlet unit theorem and standard cohomological techniques. Putting the two pieces of information together will prove the theorem.

2. The arithmetic interpretation. Using the notation of Section 1, let L be a Galois extension of a number field K with group G, and let L^* be the

Received April 15, 1963.

https://doi.org/10.1017/S002776300001120X Published online by Cambridge University Press

group of non zero elements of L. The exact sequence of G-modules

$$1 \to U_L \to L^* \to P_L \to 1$$

leads to the exact sequence of cohomology groups

$$0 \to H^0(G, U_L) \to H^0(G, L^*) \to H^0(G, P_L) \to H^1(G, U_L) \to 0$$

since Hilbert's theorem 90 tells us that $H^1(G, L^*) = 0$. For any G-module A, $H^0(G, A) = A^G$, the submodule of all elements of A left fixed by G; if A is either the group of ideals I_K, or the group of principal ideals P_K, we shall adopt the classical terminology and call the elements of A^G ambiguous ideals, or principal ambiguous ideals. The exact sequence proves

LEMMA 2.1. *$H^1(G, U_L)$ is isomorphic to the group of principal ambiguous ideals modulo those principal ideals of O_L which are generated by elements of K.*

PROPOSITION 2.2. *Let L be a Galois extension of the number field K and G be the Galois group. Let $e_1, e_2, \ldots, e_r$ be the ramification degrees of the prime ideals of K which are ramified in L. Then $[I_L^G : P^K] = e_1 e_2 \cdots e_r h_K$, where h_K is the class number of K.*

Proof. Let p be any prime ideal of K and let $P_1, P_2, \ldots, P_g$ be the prime ideal of L above p. Then

$$pO_L = (P_1 P_2 \cdots P_g)^e = A(p)^e$$

and the set of ideals $A(p)$ are easily seen to be a set of free generators for the ambiguous ideals, therefore $[I_L^G : I_K] = e_1 e_2 \cdots e_r$. Using the index relation $[I_L^G : P_K] = [I_L^G : I_K][I_K : P_K]$, one obtains the desired result.

COROLLARY 2.3. *If every ambiguous ideal is principal, then*

$$[H^1(G, U_L) : 1] = e_1 e_2 \cdots e_r h_K$$

PROPOSITION 2.4. *Let L be a Galois extension of K and let T be the Hilbert class field of L. Then T is a Galois extension of K with group G and $[H^1(G, U_T) : 1] = e_1 e_2 \cdots e_r h_K$ where e_i are the ramification degress of the primes of K which are ramified in L.*

Proof. The ideals of T which are ambiguous for the extension T/K are also ambiguous for the extension T/L. Since T/L is unramified, the proof of proposition 2.2 shows that the ambiguous ideals of T/K are extensions of·

ideals of L. We invoke the principal ideal theorem to conclude that the ambiguous ideals are principal; we may now apply corollary 2.3 noticing that the ramification degrees in T/K and in L/K are the same.

3. The cohomological interpretation. In this section, we shall obtain a bound for the order of $H^1(G, U_L)$ where L/K is a Galois extension of group G. This will be done by using standard cohomological techniques for which the reader is referred to [2, 3].

We consider first the special case where G is cyclic of prime order p. We recall that the Herbrand quotient of a G-module A is defined by

$$h(A) = [H^0(G, A): 1]/[H^1(G, A): 1]$$

where $H^0(G, A) = A^G/NA$ is the Tate cohomology group (N denotes the norm $N = \sum_{g \in G} g$). Tate's theorem [3] shows that if A is a finitely generated abelian group of rank a, and A^G is of rank b, then $h(a) = p^c$ where $c = (pb - a)/(p-1)$.

LEMMA 3.1. *Let L/K be a Galois extension with group G. Suppose G is cyclic of prime order p. Then $h(U_L) = p^{r-1}$ where r is the number of infinite primes of K which ramify in L.*

Proof. Suppose that there are s real and t complex infinite primes in K. Let r be the number of ramified infinite primes, i.e. r of the real primes become complex in L (this can occur only if $p=2$), and $s-r$ of the real primes stay real. Then the Dirichlet unit theorem shows that the rank of U_L is $p(s-r+t)+r-1$ and the rank of $U_L^G = U_K$ is $s+t-1$. Tate's theorem completes the proof.

PROPOSITION 3.2. *Let L/K be a Galois extension with group G. Suppose G is cyclic of prime order p. Let u be the number of infinite primes of K which are unramified in L. Then the order of $H^1(G, U_L)$ divides p^{u+1}. In particular, the order of $H^1(G, U_L)$ divides $p^{R(L,p)}$, where $R(L, p) = \dfrac{[L:Q]}{p} + 1$.*

Proof. The Dirichlet unit theorem shows that $U_K = W_K \times F$, where W_K is the cyclic group of roots of unity in K and F is a free abelian group of rank $s+t-1$, in the notation of the lemma.

Thus $[U_K: U_K^p]$ divides p^{s+t}. Since $N_{L/K} U_L$ contains U_K^p, it follows that $[H^0(G, U_L): 1]$ divides p^{s+t}. We now apply lemma 3.1 and the definition of the Herbrand quotient to prove the first assertion. The second comes from the inequality $u \leq [K:Q] = \frac{[L:Q]}{p}$.

Proposition 3.3. *Let L/K be a Galois extension with group G. Suppose G is of order p^n for some prime number p. Then $[H^1(G, U_L):1]$ divides $p^{R(L,p^n)}$, where*

$$R(L, p^n) = [L:Q]\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^n}\right) + n.$$

Proof. We shall apply mathematical induction on n. For $n=1$, we use the last proposition. Now, let $n>1$, then the group G is nilpotent and we may find a normal subgroup H such that G/H is cyclic of order p. Let M be the fixed field of H, then $U_L^H = U_M$ and we have the following exact sequence:

$$0 \to H^1(G/H, U_M) \to H^1(G, U_L) \to H^1(H, U_L)$$

from which we conclude that $[H^1(G, U_L):1]$ divides the product $[H^1(G/H, U_M):1][H^1(H, U_L):1]$. The induction hypothesis may now be invoked.

Proposition 3.4. *Let L/K be a Galois extension with group G of order n. Let $n = \prod_p p^{a(p)}$ be a factorization of n into prime powers. Then $[H^1(G, U_L):1]$ divides $\prod_p p^{R(L,p^{a(p)})}$ where R is the function introduced in proposition 3.3.*

Proof. Let G_p be any p-Sylow subgroup of G, then $[H^1(G_p, U_L):1]$ divides $p^{R(L,p^{a(p)})}$ by proposition 3.3. The result now follows from the fact that the restriction map,

$$\text{res}: H^1(G, U_L) \to H^1(G_p, U_L)$$

is injective on the p-primary component of $H^1(G, U_L)$.

Let $R(m, n) = \prod_p p^{R(L,p^{a(p)})}$ where $n = \prod_p p^{a(p)}$ is a factorization of n, and L is any extension of degree nm over the rationals: note that $R(m, n)$ actually depends only on m and n. The number $R(m, n)$ is the integer refered to in the statement of our Main Theorem which we are now ready to prove.

Proof of the Main Theorem. Let T be the Hilbert class field of L, then the extension T/K will be Galois with group G. If H is the subgroup corresponding to the extension T/L, then the group of G/H is the Galois group of L/K and thus is of order n. We now have the exact sequence:

$$0 \to H^1(G/H, U_L) \to H^1(G, U_T) \to H^1(H, U_T)$$

which shows that $[H^1(G, U_T) : 1]$ divides the product $[H^1(G/H, U_L) : 1]$ $[H^1(H, U_T) : 1]$. Proposition 2.4 shows that the order of $H^1(G, U_T)$ is $e_1 e_2 \cdots e_r h_K$ and that of $H^1(H, U_T)$ is h_L, while proposition 3.4 shows that the order of $H^1(G/H, U_L)$ divides $R(m, n)$. The conclusion is now immediate.

Bibliography

[1] Leopoldt, H. Sur Geschlertertheorie in abelschen Zahlkörpern, Math. Nach. Vol. **9** (1953).

[2] Serre, J. P. Cohomologie des groupes et applicatione arithmétiques, Collège de France 1958.

[3] Chevalley, Cl. Class field theory, Notes at Nagoya University 1954.

[4] Artin-Tate Class field theory, Notes by S. Lang, Harvard 1956.

Boston College
Brown University