RAMIFICATION AND CLASS TOWERS OF NUMBER FIELDS

A. Brumer

1. INTRODUCTION

In their paper settling the class tower problem, Šafarevič and Golod prove the following [2, Theorem 3].

PROPOSITION A. *Suppose that the number* r *of generators of the ideal class group of a number field* K *and the number* u *of generators of its group of units satisfy the inequality*

$$3 + 2\sqrt{u+2} \leq r.$$

Then there exists an infinite unramified p*-extension of* K, *where* p *is chosen so that the* p*-Sylow subgroup of the ideal class group of* K *has at least* r *generators.*

For the class number of an absolutely normal number field K, Rosen and the author [1] obtained lower bounds depending only on the degree and ramification indices of K. The techniques used in that paper yield similar information about the number of generators of the ideal class group of K:

PROPOSITION B. *Let* K *be a Galois extension of degree* n *over the rational field* $\underline{Q}$, *let* r *be the number of generators of its ideal class group, and suppose that* s *rational primes are ramified in* K. *Then*

$$\frac{s}{\omega(n)} - 2n \leq r,$$

where $\omega(n)$ *denotes the number of distinct prime factors of* n.

We conclude that a number field with many ramified primes has an infinite unramified extension. This complements the observation of Kuroda [3] that fields with small discriminants have no nontrivial unramified extensions. More precisely, we have the following result.

THEOREM. *Let* K *be a Galois extension of* $\underline{Q}$ *of degree* n. *Suppose that at least* $\omega(n)(3 + 2n + 2\sqrt{n+2})$ *rational primes ramify in* K. *Then the* p*-class tower of* K *is infinite for some prime* p *dividing* n.

2. PROOF OF PROPOSITION B

We shall only sketch some of the steps involved, since they differ from those in [1] only in that we are here concerned with the number of generators of the groups whose orders we computed in [1].

Let r(A) denote the *rank* of the abelian group A, that is, the number of generators of A. We formulate the following lemma as a guide to help the reader translate the proofs of [1].

Received January 22, 1965.
The author holds a T. H. Hildebrandt Research Instructorship.

LEMMA 0. i) $r(A) = \max_p r(A_p)$, *where* A_p *is the* p-*Sylow subgroup of* A.

ii) *If* A *has order* n *and* A *is the direct sum of* s *cyclic groups, then* $r(A) \geq \frac{s}{\omega(n)}$, *where* $\omega(n)$ *is the number of distinct prime divisors of* n.

iii) *Let* $f: A \to B$ *be a homomorphism; then* $r(A) \leq r(B)$ *if* f *is injective, and* $r(B) \leq r(A)$ *if* f *is surjective.*

iv) *Let* $0 \to A' \to A \to A'' \to 0$ *be an exact sequence; then*

$$\max(r(A'), r(A'')) \leq r(A) \leq r(A') + r(A'').$$

In particular, repeated application of Lemma 0 to the arguments of Section 3 in [1] yields the following.

LEMMA 1. *Let* L/K *be a Galois extension with group* G *of order* n. *Let* $n = \prod_p p^{a(p)}$ *be the factorization of* n *into prime powers. Then*

$$r(H^1(G, U_L)) \leq \max_p R(L, p^{a(p)}),$$

where U_L *is the group of units of* L *and*

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

We obtain a lower bound for the rank of $H^1(G, U_L)$ by considering its arithmetic interpretation as in Section 2 of [1].

LEMMA 2. *Let* L/K *be a Galois extension with group* G. *Suppose that every ideal of* L *invariant under* G *is principal and that* s *primes of* K *ramify in* L. *Then*

$$\max\left(\frac{s}{\omega(n)}, r(Cl_K)\right) \leq r(H^1(G, U_L)),$$

where Cl_K *is the ideal class group of* K; *if* s = 0, *equality occurs.*

Proof. We denote by A^G the group of elements of the G-module A left fixed by G. Let I_L be the group of ideals of L, and P_L the subgroup of principal ideals. The exact sequence of G-modules

$$0 \to U_L \to L^* \to P_L \to 0$$

gives, in cohomology,

$$0 \to U_K \to K^* \to P_L^G \to H^1(G, U_L) \to H^1(G, L^*) = 0.$$

Hence $H^1(G, U_L) = P_L^G/P_K = I_L^G/P_K$, since every ideal of L invariant under G is principal. Thus we have an exact sequence

$$0 \to Cl_K \to H^1(G, U_L) \to I_L^G/I_K \to 0.$$

Let q be any prime ideal of K, let $Q_1, \cdots, Q_g$ be the prime ideals of L above q, and let O_L be the ring of integers in L. Then

$$qO_L = (Q_1 \cdots Q_g)^e = A(q)^e.$$

The ideals A(q) are a set of free generators for I_L^G, hence

$$I_L^G/I_K \cong Z_{e_1} \oplus \cdots \oplus Z_{e_s},$$

where the e_i are the ramification indices of the primes of K ramified in L, and where Z_{e_i} is the cyclic group of order e_i. An application of (ii) and (iv) of Lemma 0 completes the proof.

Proof of Proposition B. Let L be the Hilbert class field of K; then L is a Galois extension of $\underline{Q}$ with group G. Let H be the Galois group of L over K. Since L is an unramified extension of K, every ideal of L invariant under H (and *a fortiori* under G) comes from K and thus is principal by the principal ideal theorem. We have the exact sequence

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

hence

$$r(H^1(G, U_L)) - r(H^1(G/H, U_K)) \leq r(H^1(H, U_L)).$$

The conclusion follows if we apply Lemma 2 to the first and third term and Lemma 1 to the second term, after using the very crude estimate $R(K, p^m) < 2n$.

REFERENCES

1. A. Brumer and M. Rosen, *Class number and ramification in number fields*, Nagoya Math. J. 23 (1963), 97-101.

2. E. S. Golod and I. R. Šafarevič, *On the class field tower*, Izv. Akad. Nauk. SSSR Ser. Mat. 28 (1964), 261-272.

3. S. Kuroda, *On a theorem of Minkowski*, Sûgaku 14 (1962/63), 171-172.

The University of Michigan