GALOIS GROUPS OF EXTENSIONS OF ALGEBRAIC NUMBER FIELDS WITH GIVEN RAMIFICATION

Armand Brumer

Let k be an algebraic number field, and let S be a set of valuations on k. Let G be the Galois group of the maximal extension of k unramified outside of S. Šafarevič [10] has pointed out the interest and importance of this group. It will be shown here that the cohomological p-dimension of G is at most 2 *if* S *contains all primes above* p *and if, in addition,* k *is totally imaginary in case* p = 2; this generalizes a result of Tate in case S consists of all primes of k [11, Chapter II]. As a consequence, the Galois group P of the maximal p-extension of k unramified outside S is a pro-p-group of cohomological dimension at most two. (In a paper to appear in the Journal of Algebra, the author studies profinite groups of finite cohomological dimension. A single group-theoretic criterion shows that the groups we consider here have strict cohomological dimension 2.) In the final section, we compute the number of generators and relations for the group P in case k contains the pth roots of unity; this completes, in the situation we consider, a result of Šafarevič [10]. In particular, we find necessary and sufficient conditions for P to be free, and thereby we prove anew a result of Iwasawa [6] on regular cyclotomic extensions.

The author wishes to express his gratitude to Jean-Pierre Serre for having taught him this subject *in absentia* through his lecture notes, and to John Smith for many stimulating discussions. The author also thanks the referee for pointing out that Tate [12] has announced deep results (whose proofs still remain unpublished) that include many of those obtained here by more elementary means.

1. NOTATION AND A TRANSITIONAL LEMMA

We use freely the language of profinite groups, that is, compact, totally disconnected topological groups (for a convenient source, see [5]; a more complete treatment is given in [11]). The class field theoretic results we need can all be found in [1].

We consider an algebraic number field M (not necessarily finite) and a set S of valuations on M. We shall also use the letter S to denote, by *abus de langage*, the set of valuations on a Galois extension Ω of M whose restrictions to M fall into S. We say that Ω/M is *unramified outside of* S if every valuation of Ω not in S is unramified over M. We say that Ω/M is (S, p)-*closed* if in addition every proper p-extension of Ω ramifies outside of S. This is most conveniently expressed as follows. Let K_S be the subring of K consisting of fractions a/b, where a and b are integers in K and b is a unit outside S; in other words, let K_S be the intersection of all valuation rings of K whose primes do not fall into S. Then Ω/M is unramified outside S if and only if Ω_S/M_S is a Galois extension of commutative rings in the sense of Auslander and Goldman [3]. In [2] only the case in which the Galois group

Received April 23, 1965.
This work was completed while the author was a T. H. Hildebrandt Research Instructor at the University of Michigan.

is finite was considered, but the passage to the limit causes no problem. The group of units $U(K_S)$ of K_S is simply the so-called group of S-units of K. The reader should note that there may be ramification on the set S_∞ of infinite primes.

LEMMA 1.1. *Let* M *be a number field, and let* S *be any set of valuations of* M *containing all valuations above* p. *Let* L *be an* (S, p)*-closed extension of* M *containing the group* μ_p *of* pth *roots of unity. Then we have an exact sequence*

$$1 \to \mu_p \to U(L_S) \overset{p}{\to} U(L_S) \to 1,$$

where p *denotes the* pth *power map.*

Proof. It is well known [1, Chapter 6, Theorem 4] that the adjunction of the pth root of an S-unit introduces no ramification outside S.

LEMMA 1.2. *With the same notation as above, let* G *be the Galois group of* L/M. *Then the following are equivalent.*

i) $\mathrm{cd}_p\, G \leq n$.

ii) *For every extension* K *of* M *unramified outside* S, $H^n(H, U(L_S))$ *is divisible by* p *and* $H^{n+1}(H, U(L_S))(p) = 0$, *where* H *is the Galois group of* L *over* K. (For any abelian group A, we write A(p) for the p-primary component of A.)

iii) *The same as* ii), *except that we consider only extensions* K/M *that are finite extensions of degree relatively prime to* p.

Proof. From Lemma 1.1, we see that condition ii) is equivalent to $H^{n+1}(H, \mu_p) = 0$. We complete the proof by copying that of Proposition 4 in Chapter II of [11], which it generalizes.

We must thus interpret the cohomology of the group of S-units: this is the content of the next section.

2. COHOMOLOGY OF THE GROUP OF S-UNITS

Auslander and the author [2], and independently Chase, Harrison, and Rosenberg [4], have found a seven-term exact sequence that holds for Galois extensions of commutative rings. We apply this result to obtain the following.

PROPOSITION 2.1. *Let* L *be a Galois extension of* K, *unramified outside* S, *with group* G. *Then we have an exact sequence*

$$0 \to H^1(G, U(L_S)) \to \mathbb{P}(K_S) \to H^0(G, \mathbb{P}(L_S)) \to H^2(G, U(L_S))$$
$$\to B(L_S/K_S) \to H^1(G, \mathbb{P}(L_S)) \to H^3(G, U(L_S)),$$

where $\mathbb{P}(L_S)$ *denotes the projective class group of* L_S *and* $B(L_S/K_S)$ *is the subgroup of the Brauer group of* K_S *split by* L_S.

Proof. We have already observed that L_S is a Galois extension of K_S, hence the results mentioned above are directly applicable.

Remark 2.2. If K is a finite number field, $\mathbb{P}(K_S)$ may be identified with the quotient of the ideal class group Cl_K of K by the subgroup generated by the classes of all primes in S. If K is an infinite extension, then $\mathbb{P}(K_S) = \varinjlim \mathbb{P}((K_i)_S)$, where the K_i are finite extensions with $K = \varinjlim K_i$.

PROPOSITION 2.3. *Let* L *be an* (S, p)-*closed extension of* K, *and let* G *be the Galois group of* L *over* K. *Then*

i) $H^1(G, U(L_S))(p) = \mathbb{P}(K_S)(p)$,

ii) $H^2(G, U(L_S))(p) = B(L_S/K_S)(p)$.

Proof. It is readily verified (see Section 6 of [8]) that we may write $L = \varinjlim L_i$ and $K = \varinjlim K_i$, where L_i is a Galois extension of K_i unramified outside S and L_i is a finite number field. Since L is an (S, p)-closed extension of K, we conclude that L contains the maximal abelian unramified p-extension of L_i, for each i. The principal ideal theorem shows that $\varinjlim \mathrm{Cl}_{L_i}(p) = 0$; hence it follows that $\mathbb{P}(L_S)(p) = 0$, by Remark 2.2. An alternative proof of this result, under the hypothesis that S contains all primes above p, is given in the Appendix. The result follows from Proposition 2.1, if we take p-primary components.

Let K be the union of finite number fields K_i. For any valuation v of K, denote by K_v the direct limit of the finite completions $(K_i)_v$; that is, let $K_v = \varinjlim (K_i)_v$. We define the *local degree* at v to be the least common multiple of $[(K_i)_v : \mathbb{Q}_v]$ in the sense of supernatural numbers. At this point it is convenient to recall a result contained in the proof of Proposition 9, Chapter II of [11].

LEMMA 2.4. *Let* K *be a number field. Suppose that the local degree of every valuation is divisible by* p^∞ *and that* K *is totally imaginary in case* p = 2. *Then* B(K)(p) = 0, *where* B(K) *is the Brauer group of* K. *In particular,* $B(K_S)(p) = 0$.

Proof. Since K_S is the direct limit of Dedekind domains, the natural map $B(K_S) \to B(K)$ is a monomorphism by Theorem 7.2 of [3]. This proves the second assertion.

COROLLARY 2.5. *Let* K *have the properties in Lemma* 2.4, *and let* S *be a set of valuations including all those extending* p. *Let* L *be an* (S, p)-*closed extension of* K *containing the* p*th roots of unity, and let* G *be the Galois group of* L *over* K. *Then the following are equivalent:*

i) $\mathrm{cd}_p G \leq 1$,

ii) $\mathbb{P}(K_S)$ *is* p-*divisible.*

Proof. The p-primary component of the Brauer group of K_S is trivial, by Lemma 2.4. The result follows from Proposition 2.3 and Lemma 1.2.

Remark 2.6. The verification of ii) seems to be very difficult, and we shall use the corollary only in case $\mathbb{P}(K_S)$ is trivial. An interpretation of $\mathbb{P}(K_S)$ is given in [7].

Remark 2.7. When S contains all primes above p, Proposition 2.3 shows that

$$H^2(G, U(L_S))(p) = B(K_S)(p)$$

for any number field K.

In fact, adjoining the p^nth roots of unity introduces no ramification outside S. Since L is (S, p)-closed, it contains the subfield of order p^{n-1} of the cyclotomic field of p^nth roots of unity. Hence L satisfies the hypotheses of Lemma 2.4, and thus $B(L_S)(p) = 0$, which implies that $B(L_S/K_S)(p) = B(K_S)(p)$.

LEMMA 2.8. *Let* K *be a finite number field, and let* S *be a nonempty set of finite primes; then we have an exact sequence*

$$0 \to B(K_S) \to \bigoplus_{q \in S \cup S_\infty} B(\hat{K}_q) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where $\hat{K}_q$ *denotes the completion of* K *at the finite or infinite prime* q, *and* S_∞ *denotes the set of infinite primes of* K.

Proof. Let Λ be a central separable algebra over K_S; then Λ may be considered as a maximal order in the central simple algebra $\Lambda \otimes_{K_S} K$ over K [3]. The assumption about Λ asserts that $\Lambda \otimes_{K_S} K$ is unramified outside S. The result follows from the definition of the Hasse invariant for the Brauer group of number fields together with the observation that the map $\Lambda \to \Lambda \otimes_{K_S} K$ induces a monomorphism of $B(K_S) \to B(K)$.

From Remark 2.7 and Lemma 2.8 we obtain the following.

COROLLARY 2.9. *Let* K *be a finite number field, and let* S *be a set of primes including all primes above* p. *Let* L *be an* (S, p)*-closed extension of* K *with group* G. *Then we have an exact sequence*

$$0 \to H^2(G, U(L_S))(p) \to \bigoplus_{q \in S \cup S_\infty} B(\hat{K}_q)(p) \to \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

In particular, $H^2(G, U(L_S))$ *is divisible by* p, *if in addition* K *is totally imaginary in case* p = 2.

PROPOSITION 2.10. *Under the hypotheses of Corollary* 2.9,

$$H^3(G, U(L_S))(p) = 0.$$

Proof. Since the local degrees of L are divisible by p^∞, we conclude from Theorem 14, p. 69 of [1] that $H^3(G, L^*)(p) = 0$, where L^* denotes the multiplicative group of L. Let I_L denote the group of invertible ideals of L_S, and let H_L be the subgroup of principal ideals. Then we have two exact sequences

$$0 \to H_L \to I_L \to \mathbb{P}(L_S) \to 0,$$

$$0 \to U(L_S) \to L^* \to H_L \to 0.$$

Passing to cohomology, we obtain the sequences

(2.10.1) $H^2(G, L^*)(p) \to H^2(G, H_L)(p) \to H^3(G, U(L_S))(p) \to H^3(G, L^*)(p) = 0,$

(2.10.2) $0 \to H^2(G, H_L)(p) \to H^2(G, I_L)(p) \to 0,$

where the extreme terms in (2.10.2) are trivial, since $\mathbb{P}(L_S)(p) = 0$, as we saw in the proof of Proposition 2.3.

Let M be a finite Galois extension of K, with group H, and contained in L. We denote by J_M^S the group of ideles of M whose components are 1 at all primes of S, and by V_M^S the subgroup of J_M^S consisting of those ideles whose components are units everywhere. We have an exact sequence

$$1 \to V_M^S \to J_M^S \xrightarrow{\phi} I_M^S \to 1,$$

where $\phi((\chi_q)) = \prod q^{\nu_q(\chi_q)}$ and ν_q is the exponential valuation at the prime q. Since M is an unramified extension of K, the cohomology of V_M^S is trivial, and in particular,

$$H^2(H, I_M^S) \cong \bigoplus_{q \notin S} H^2(H_q, \hat{M}_q),$$

where q ranges through the primes of K and $\hat{M}_q$ is the completion of M at some prime above q whose decomposition group is written H_q (for details see the prologue to [1]). We may pass to the limit by choosing a valuation v of L above each prime q of K not in S. Then we have an isomorphism

$$H^2(G, I_L^S) \cong \bigoplus_{q \notin S} H^2(G_q, L_v), \tag{2.10.3}$$

which may be composed with (2.10.1) and (2.10.2) to give the exact sequence

$$H^2(G, L^*)(p) \xrightarrow{\tau} \bigoplus_{q \notin S} H^2(G_q, L_v)(p) \to H^3(G, U(L_S))(p) \to 0,$$

where the map τ is the natural map of the Brauer group of K into the direct sum of the Brauer groups of the completions of K. Since S is nonempty, and elements of $H^2(G, L^*)(p)$ are determined by their local invariants and the sole condition that the sum of these invariants be zero, we see that τ must be onto and that $H^3(G, U(L_S))(p) = 0$.

We are now ready to state and prove the main result of this section.

THEOREM 2.11. *Let* K *be a finite number field, and let* S *be a set of primes on* K *containing all primes above* p. *In case* p = 2, *suppose that* K *is totally imaginary. Let* L *be an* (S, p)-*closed extension of* K, *and let* G *be its Galois group. Then* $\mathrm{cd}_p\, G \leq 2$.

Proof. Let M be the maximal extension of K unramified outside S. Then M contains the pth roots of unity, and the hypotheses of Lemma 1.2 are satisfied because of Corollary 2.9 and Proposition 2.10. Hence $\mathrm{cd}_p\, H \leq 2$, where H is the Galois group of M over K.

Denote by N the Galois group of M over L. Then $\mathrm{cd}_p\, N \leq 1$, by Corollary 2.5, since $\mathbb{P}(L_S)(p) = 0$, as we have seen earlier. But G = H/N, and N has no proper p-quotients; hence it follows from the Hochschild-Serre spectral sequence that $\mathrm{cd}_p\, G = \mathrm{cd}_p\, H/N \leq \mathrm{cd}_p\, H \leq 2$, as in Proposition 2 of Chapter II of [11].

3. GENERATORS AND RELATIONS

In this section, we suppose K is a finite number field containing the pth roots of unity. We denote by S a set of finite primes of K containing all primes above p. Let L be the maximal p-extension of K unramified outside S, and let G be its Galois group. We wish to compute the number of generators and relations of G, that is, the dimension of $H^1(G, F_p)$ and $H^2(G, F_p)$ over the field F_p of p elements (see [9], [10], or [11]).

Once more we exploit the cohomology of the exact sequence

$$1 \to \mu_p \to U(L_S) \xrightarrow{p} U(L_S) \to 1,$$

where μ_p is the group of pth roots of unity, to obtain the exact sequences

$$(3.1.1) \qquad \begin{cases} 0 \to {}_pU(K_S) \to H^1(G, \mu_p) \to H^1(G, U(L_S))_p \to 0, \\ 0 \to {}_pH^1(G, U(L_S)) \to H^2(G, \mu_p) \to H^2(G, U(L_S))_p \to 0, \end{cases}$$

where for any abelian group A, we write $A_p = \{a \in A \mid pa = 0\}$ and ${}_pA = A/pA$. Since G is a pro-p-group, it acts trivially on μ_p; that is, $\mu_p = F_p$. We may reinterpret (3.1.1), by means of Proposition 2.3 and Corollary 2.9, to obtain the following.

THEOREM 3.1. *Let* K *and* S *be as above, and let* G *be the Galois group of the maximal* p*-extension of* K *unramified outside* S. *Then we have the exact sequences*

$$0 \to {}_pU(K_S) \to H^1(G, F_p) \to \mathbb{P}(K_S)_p \to 0,$$

$$0 \to {}_p\mathbb{P}(K_S) \to H^2(G, F_p) \to \bigoplus_{q \in S \cup S_\infty} B(\hat{K}_q)_p \xrightarrow{\sigma} F_p \to 0,$$

where $B(\hat{K}_q)$ *is the Brauer group of the completion of* K *at* q, *and* σ *is the sum of the local invariants.*

Remark. The second sequence expresses roughly the fact that the relations on G come from the local fields and the ideal class group. (In a recent conversation, James Ax mentioned that Koch has made this statement precise, in a paper to appear in J. Reine Angew. Math.) It is worthwhile to recall that $\mathbb{P}(K_S)$ is the quotient of the ideal class group of K by the subgroup generated by the classes of ideals in S; in particular, $\mathbb{P}(K_S) = \{1\}$ if S contains a prime in each ideal class of K.

We denote by $\pi(A)$ the minimal number of generators of the p-primary component A; that is, $\pi(A) = \dim_{F_p}(A_p) = \dim_{F_p}({}_pA)$.

COROLLARY 3.2. *With the notation above,* G *is a pro-*p*-group on* $|S| + r_1 + r_2 + \pi(\mathbb{P}(K_S))$ *generators with* $|S| + \pi(\mathbb{P}(K_S)) + r_1 - 1$ *relations, where* r_1 *is the number of real primes and* r_2 *the number of complex primes of* K.

Proof. The result follows from Theorem 3.1 and the Dirichlet-Hasse-Chevalley theorem on S-units, if we count dimensions over F_p.

Remark. Corollary 3.2 shows that, under our hypotheses on K and S, the upper bound obtained by Šafarevič [9] is actually equal to the number of relations of G.

COROLLARY 3.3. *Under the hypotheses of Corollary* 3.2, *the following are equivalent:*

i) G *is a free pro-*p*-group.*

ii) K *is totally imaginary, there is a unique prime* $\mathfrak{p}$ *in* K *above* p, $S = \{\mathfrak{p}\}$, *and the subgroup generated by the class of* $\mathfrak{p}$ *contains the* p*-primary component of the ideal class group of* K.

Proof. G is free if and only if it has no relations. From Corollary 3.2 we conclude that $|S| = 1$ and $\mathbb{P}(K_S)(p) = 0$; hence our result follows.

Remark. Since a closed subgroup of a free pro-p-group is also free, we conclude that property ii) is inherited by p-extensions L of K unramified outside p. This applies, in particular, if p is a regular prime and K is the cyclotomic field of pth roots of unity (respectively, $\mathbb{Q}(i)$), in which case we conclude that G is a free pro-p-group on $(p+1)/2$ (respectively, 2) generators. We also recover the fact that p does not divide the class number of the cyclotomic field of p^nth roots of unity, since the unique prime $\mathfrak{p}$ above p is principal (see [6]).

4. APPENDIX

Let R be a Dedekind domain, containing the pth roots of unity, and in which p is a unit; and let K be the quotient field of R. Let L be an extension of K, closed under unramified p-extensions. Then $\mathbb{P}(T)(p) = \{1\}$, where T is the integral closure of R in L. In fact, choose an invertible ideal $\mathfrak{A}$ of order p in $\mathbb{P}(T)$, so that $\mathfrak{A}^p = (\mu)$ with $\mu \in L$. Then $\mathfrak{A}$ and μ come from a finite extension of K, and we may suppose without loss of generality that they come from K. Since $\mathfrak{A}^p = (\mu)$, p divides the exponential valuation of μ at every prime q of R. Since p is a unit in R, we verify easily that $K(\sqrt[p]{\mu})$ is an unramified extension of K, for instance by localization. Hence $K(\sqrt[p]{\mu})$ is contained in L, and $\mathfrak{A} = (\sqrt[p]{\mu})$; that is, $\mathfrak{A}$ is principal, and our claim follows.

This result shows that we did not need the principal ideal theorem for our applications.

REFERENCES

1. E. Artin and J. Tate, *Class field theory*, Lithographed notes, Institute for Advanced Study, Princeton, 1961.

2. M. Auslander and A. Brumer, *Galois cohomology and the Brauer group of commutative rings* (unpublished).

3. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. 97 (1960), 367-409.

4. S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965).

5. A. Douady, *Cohomologie des groupes compact totalement discontinus*, Séminaire Bourbaki, 1959-60, exposé 189.

6. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257-258.

7. ———, *Sheaves for algebraic number fields*, Ann. of Math. (2) 69 (1959), 408-413.

8. ———, *On Γ-extensions of number fields*, Bull. Amer. Math. Soc. 65 (1959), 183-226.

9. I. R. Šafarevič, *On algebraic number fields* (in Russian), Proc. Internat. Congress Math. pp. 163-176. Stockholm, 1963.

10. ———, *Extensions with given ramification points* (in Russian), Publ. Math. Institut des Hautes Études Scientifiques, No. 18, 1963.

11. J.-P. Serre, *Cohomologie Galoisiènne*, Collège de France, Springer Lecture Series No. 5, 1963.

12. J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congress Math. 1962, 288-295. Stockholm, 1963.

The University of Michigan