Can. J. Math., Vol. XXIII, No. 3, 1971, pp. 398–402

THE MAXIMAL p-EXTENSION OF A LOCAL FIELD

MURRAY A. MARSHALL

1. Let k denote a local field, that is, a complete discrete-valued field with perfect residue class field $\bar{k}$. Let G denote the Galois group of the maximal separable algebraic extension M of k, and let g denote the corresponding object over $\bar{k}$. For a given prime integer p, let $G(p)$ denote the Galois group of the maximal p-extension of k. The dimensions of the cohomology groups

$$H^q(G(p), \mathbf{Z}/p\mathbf{Z}), \; q = 1, 2,$$

considered as vector spaces over the prime field $\mathbf{Z}/p\mathbf{Z}$, are equal, respectively, to the rank and the relation rank of the pro-p-group $G(p)$; see [**4**; **9**]. These dimensions are well known in many cases, especially when $\bar{k}$ is finite [**6**; **3**; (Hoechsmann) **2**, pp. 297–304], but also when k has characteristic p, or when k contains a primitive pth root of unity [**4**, p. 205].

Our aim in this article is to indicate a uniform method for computing $H^q(G, \mathbf{Z}/p\mathbf{Z})$, $q = 1, 2$, which applies whenever g has cohomological p-dimension less than two. Moreover, it is shown that if k has at least one totally ramified cyclic p-extension, then $H^2(G(p), \mathbf{Z}/p\mathbf{Z}) \cong H^2(G, \mathbf{Z}/p\mathbf{Z})$. (The corresponding result in dimension one is trivial.)

With these goals in mind, the following additional notation is introduced. For the prime p considered above, let S denote the group of pth roots of unity in T, where T denotes the maximal unramified extension of k. Further, let H denote the kernel of the natural homomorphism of G onto g. (Thus H is the Galois group of M over T.) If v denotes the valuation on M normalized to k, then define $e = v(p)$, and $s = ep(p-1)$. (e satisfies $0 \leqq e \leqq \infty$, and in the case that $e = \infty$, we understand that s is also ∞.) If K is any pro-finite group, then $\mathbf{Z}/p\mathbf{Z}$ is a K-module under the trivial action, and the cohomology groups $H^q(K, \mathbf{Z}/p\mathbf{Z})$, $q \geqq 0$, will be denoted simply by $H^q(K)$.

Let h denote the Galois group of the maximal elementary p-extension of T. Let h^x, $x \in R$, denote the ramification subgroups of h. (See [**1**, pp. 119–120], for the definition of ramification for infinite extensions.) By the theorem of Hasse and Arf [**7**, p. 84], the jumps of the filtration $\{h^x: x \in R\}$ are integers, and so the filtration has the form

$$h = h^1 \supseteq h^2 \supseteq h^3 \supseteq \ldots . \tag{1}$$

Taking the completion of T, we may assume, without loss of generality, that T

Received May 7, 1970.

is complete under v; then the structure of the filtration (1) is given by local class field theory [8]. We have

(2) (a) $h^n = h^{n+1}$ if $0 < n < s$, and $p|n$;
(b) $h^s \cong S$ canonically;
(c) $H^1(h^n/h^{n+1}) \cong \bar{T}$, if $0 < n < s$, $p \nmid n$.

It should be noted that these mappings may be given explicitly as follows.

In the non-trivial case, $\text{ord}(h^s) = \text{ord}(S) \neq 1$, the isomorphism $h^s \to S$ is given by $\sigma \to \sigma(\pi)^{1/p}/(\pi)^{1/p}$, where π is a prime of T (see [8, § 4.3]). This mapping is independent of the choice of π.

The isomorphism $\bar{T} \to H^1(h^n/h^{n+1})$ is given as follows. Let $\bar{u} \neq 0$, $\bar{u} \in \bar{T}$. Let $y = 1 + u\pi^{-n}$, where π is a fixed prime of T. Choose $x \in M$ to satisfy $x^p - x = y$, and let $L = T(x)$. Then $L|T$ is cyclic of degree p with a single jump n, and if $\sigma \in h^n$, then $\sigma x - x$ is an integer of L, and its image in the residue class field $\bar{L} = \bar{T}$ is actually in the prime field $\mathbf{Z}/p\mathbf{Z}$. Define

$$\chi\colon h^n/h^{n+1} \to \mathbf{Z}/p\mathbf{Z} \text{ by } \chi(\bar{\sigma}) = \overline{\sigma x - x}.$$

Then $\bar{u} \to \chi$ is the required isomorphism (see [8, § 4.4]).

Since $g = G(T|k) = G(\bar{T}|\bar{k})$, T and $\bar{T}$ are naturally g-modules. Clearly S is a g-submodule of T; the action of g on S being trivial if and only if $S \subseteq k$. g also acts on the groups h^n/h^{n+1} and h^s by inner automorphism. In this way, $H^1(h^n/h^{n+1}) = \text{Hom}(h^n/h^{n+1}, \mathbf{Z}/p\mathbf{Z})$ becomes a g-module in the standard way. We note the following important fact. If π is chosen to be a prime in k, then the isomorphisms of (2) are g-module isomorphisms.

THEOREM 1. *Suppose that $cd_p(g) \leqq 1$. Then*
(a) $H^1(G) \cong H^1(g) \oplus (\bigoplus_{i=1}^{e} \bar{k}_i) \oplus H^1(S^g)$, *and*
(b) $H^2(G) \cong H^1(g, H^1(S))$ *canonically.*
(*Here $\bar{k}_i$ denotes a copy of the additive group $\bar{k}$.*)

Proof. One notes readily that there are e integers n satisfying $0 < n < s$, $p \nmid n$. If n is any such integer, then by (2)(c) we have the exact sequence of g-modules:

$$0 \to \bar{T} \to H^1(h^n) \to H^1(h^{n+1}) \to 0.$$

Applying the cohomology sequence together with the well-known fact that $H^q(g, \bar{T}) = 0$ for all $q \geqq 1$, we obtain the following sequences:

$$0 \to \bar{k} \to H^1(h^n)^g \to H^1(h^{n+1})^g \to 0, \tag{3}$$

$$0 \to H^1(g, H^1(h^n)) \to H^1(g, H^1(h^{n+1})) \to 0. \tag{4}$$

The sequence (3) splits, since the groups are elementary p-groups. Thus, combining (2) and (3) we obtain

$$H^1(h)^g \cong \bigoplus_{i=1}^{e} \bar{k}_i \oplus H^1(S)^g. \tag{5}$$

https://doi.org/10.4153/CJM-1971-041-8 Published online by Cambridge University Press

On the other hand, combination of (2) and (4) yields

$$(6) \qquad H^1(g, H^1(h)) \cong H^1(g, H^1(h^s)) \cong H^1(g, H^1(S)).$$

The exact sequence

$$0 \to H \to G \to g \to 0$$

yields the 5-term exact sequence

$$(7) \qquad 0 \to H^1(g) \xrightarrow{\text{inf}} H^1(G) \xrightarrow{\text{res}} H^1(H)^g \xrightarrow{\text{tr}} H^2(g) \xrightarrow{\text{inf}} H^2(G)$$

(see [**4** or **9**]). Since $cd_p(g) \leqq 1$, we have $H^2(g) = 0$; thus (7) yields

$$(8) \qquad H^1(G) \cong H^1(g) \oplus H^1(H)^g.$$

Since $H^1(H) = H^1(h)$ and $H^1(S)^g = H^1(S^g)$, combining (5) and (8) we obtain (a).

To prove (b), recall that the Brauer group is trivial over finite extensions of T; see [**7**]. By the results in [**4**, pp. 203–206], this yields $cd_p(H) \leqq 1$. Thus, by the theory of spectral sequences [**4**, p. 208], we have

$$(9) \qquad H^2(G) \cong H^1(g, H^1(H)).$$

Combining (6) and (9), we obtain (b).

In view of the introductory remarks, we really wish to compute $H^q(G(p))$, $q = 1, 2$, rather than $H^q(G)$. Of course, $H^q(G(p)) = H^q(G)$ when $q = 1$. The following lemma prepares the way for a corresponding result in the case $q = 2$.

LEMMA. *Suppose that k_i is a local field and that G_i and g_i are defined as above, $i = 1, 2$. Further, suppose that $k_2|k_1$ is cyclic totally ramified of degree p, and that $cd_p(g_i) \leqq 1$, $i = 1, 2$. Then the natural restriction homomorphism*

$$\text{Res: } H^2(G_1) \to H^2(G_2)$$

is trivial.

Proof. We have

$$H^2(G_i) \cong H^1(g_i, H^1(H_i)) \cong H^1(g_i, H^1(h_i)), \qquad i = 1, 2.$$

Let π_i denote a prime of k_i, $i = 1, 2$. Then by the hypothesis, $\pi_1 = u\pi_2^p$, where u is a unit of k_2. Let $L = T_1((\pi_1)^{1/p})$. Then $LT_2 = T_2((u)^{1/p})$, and so the jump of $LT_2|T_2$ is less than $s_2 = e_2p/(p-1)$ [**10**, p. 143]. Thus, the natural mapping $h_2 \to h_1$ factors through h_2/S; and so, in turn, the natural mapping

$$\text{Res: } H^1(g_1, H^1(h_1)) \to H^1(g_2, H^1(h_2))$$

factors through $H^1(g_2, H^1(h_2/S)) = 0$.

THEOREM 2. *Assume that $cd_p(g) \leqq 1$. If k has no totally ramified cyclic p-extensions, then $H^2(G(p)) = 0$. Otherwise,*

$$H^2(G(p)) \cong H^2(G)$$

canonically.

https://doi.org/10.4153/CJM-1971-041-8 Published online by Cambridge University Press

Proof. The condition that k has no totally ramified cyclic p-extensions is clearly equivalent to the equality $G(p) = g(p)$, and the result comes immediately from the assumption that $cd_p(g) \leqq 1$; see [**4**, p. 201].

To prove the second assertion, let K denote the kernel of the natural homomorphism of G onto $G(p)$. Since $G(p)$ is the maximal p-factor group of G, we have $H^1(K) = 0$, and so we obtain the exact sequence

$$0 \to H^2(G(p)) \xrightarrow{\text{inf}} H^2(G) \xrightarrow{\text{res}} H^2(K).$$

But by the lemma, this restriction is trivial. This completes the proof.

2. Applications. The most interesting prime is $p = \text{char}(\bar{k})$. In this case, $cd_p(g) \leqq 1$, and so Theorems 1 and 2 apply. Theorem 1 yields the rank formula:

$$\text{rank}\, G(p) = \text{rank}\, g(p) + ef + \text{rank}\, S^g,$$

where f denotes the dimension of $\bar{k}$ as a vector space over $\mathbf{Z}/p\mathbf{Z}$. The results concerning the relation rank may be interpreted in several cases.

(1) The condition that $S = 1$ is equivalent to the condition that $s = ep/(p-1)$ is not an integer (i.e. it is a rational number or infinity); see [**9**, p. 114]. In this case $G(p)$ is a free pro-p-group.

(2) Suppose that $S^g \neq 1$. Thus g operates trivially on $S = S^g$, and hence

$$H^2(G(p)) \cong H^1(g, H^1(S)) \cong H^1(g) \cong \bar{k}/\mathscr{P}(\bar{k}),$$

where $\mathscr{P}(x) = x^p - x$. Thus $G(p)$ is a free pro-p-group if and only if $\bar{k}$ has no cyclic p-extensions. This result may also be derived in a more direct manner using Kummer theory; see Hoechsmann [**2**, pp. 297–304].

(3) Suppose that $S \neq 1$, $S^g = 1$. Let $k_1 = k(S)$, let $(\tau) = G(k_1|k)$, and suppose that $i \in \mathbf{Z}/p\mathbf{Z}$ is defined by $\omega^\tau = \omega^i$ for $\omega \in S$. Then

$$\begin{aligned} H^2(G(p)) \cong H^1(g, H^1(S)) &\cong H^1(G(T|k_1), \quad H^1(S))^{(\tau)} \\ &\cong H^1(G(T|k_1))^{\tau-i} \cong (\bar{k}_1/\mathscr{P}(\bar{k}_1))^{\tau-i}, \end{aligned}$$

where $A^{\tau-i} = \{a \in A : a^\tau = a^i\}$. Thus, $H^2(G(p))$ corresponds to a certain class of non-Galois extensions of degree p over $\bar{k}$. In particular, $G(p)$ will be free if $\bar{k}$ has only abelian p-extensions, as in the quasi-finite case.

Let $p = \text{char}(\bar{k})$, and let A denote the Galois group of the maximal abelian extension of k. Clearly $A(p)$ is a free abelian pro-p-group if $cd_p(G(p)) \leqq 1$. The converse may also be shown, and in this case, the topological group A, together with its ramification subgroups

$$A \supseteq A^0 \supseteq A^1 \supseteq A^2 \supseteq \ldots \supseteq A^n \supseteq A^{n+1} \supseteq \ldots,$$

is completely characterized as a topological filtered group; see [**5**, pp. 142–143].

References

1. E. Artin and J. Tate, *Class field theory* (Benjamin, New York, 1967).
2. J. W. S. Cassels and A. Froehlich, *Algebraic number theory* (Thompson Book Co., Washington, D.C., 1967).

3. S. P. Demuškin, *The group of a maximal p-extension of a local field*, Izv. Akad. Nauk SSSR Ser. Mat. *25* (1961), 329–346.
4. S. Lang, *Rapport sur la cohomologie des groupes* (Benjamin, New York, 1966).
5. M. A. Marshall, *The ramification filters of abelian extensions of a local field*, Queen's University Preprint 1969-6, Kingston, Ontario.
6. I. R. Šafarevič, *On p-extensions*, Mat. Sb. (N.S.) *20* (*62*), (1947), 351–363.
7. J.-P. Serre, *Corps locaux* (Hermann, Paris, 1962).
8. ——— *Sur les corps locaux à corps résiduel algébricquement clos*, Bull. Soc. Math. France *89* (1961), 105–154.
9. ——— *Cohomologie galoisienne* (Springer-Verlag, Berlin, 1965).
10. B. F. Wyman, *Wildly ramified gamma extensions*, Amer. J. Math. *91* (1969), 135–152.

University of Saskatchewan,
Saskatoon, Saskatchewan