COHOMOLOGICAL DIMENSION AND SCHREIER'S FORMULA IN GALOIS COHOMOLOGY

JOHN LABUTE, NICOLE LEMIRE†, JÁN MINÁČ‡, AND JOHN SWALLOW

Abstract. Let p be a prime and F a field containing a primitive pth root of unity. If $p > 2$ assume also that F is perfect. Then for $n \in \mathbb{N}$, the cohomological dimension of the maximal pro-p-quotient G of the absolute Galois group of F is n if and only if the corestriction maps $H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ are surjective for all open subgroups H of index p. Using this result we derive a surprising generalization to $\dim_{\mathbb{F}_p} H^n(H, \mathbb{F}_p)$ of Schreier's formula for $\dim_{\mathbb{F}_p} H^1(H, \mathbb{F}_p)$.

For a prime p, let $F(p)$ denote the maximal p-extension of a field F. One of the fundamental questions in the Galois theory of p-extensions is to discover useful interpretations of the cohomological dimension $\mathrm{cd}(G)$ of the Galois group $G = \mathrm{Gal}(F(p)/F)$ in terms of the arithmetic of p-extensions of F. When $\mathrm{cd}(G) = 1$, for instance, we know that G is a free pro-p-group [S1, §3.4], and when $\mathrm{cd}(G) = 2$ we have important information on the G-module of relations in a minimal presentation [K, §7.3].

For a fixed $n > 2$, however, little is known about the structure of p-extensions when $\mathrm{cd}(G) = n$. Now when $n = 1$ and G is finitely generated as a pro-p-group, we have Schreier's well-known formula

$$h_1(H) = 1 + [G : H](h_1(G) - 1) \tag{1}$$

for each open subgroup H of G, where

$$h_1(H) := \dim_{\mathbb{F}_p} H^1(H, \mathbb{F}_p).$$

(See, for instance, [K, Example 6.3].)

Date: November 17, 2004.

2000 *Mathematics Subject Classification.* Primary 12G05, 12G10.

Key words and phrases. cohomological dimension, Schreier's formula, Galois theory, p-extensions, pro-p-groups.

†Research supported in part by NSERC grant R3276A01.

‡Research supported in part by NSERC grant R0370A01, by the Mathematical Sciences Research Institute, Berkeley, and by a 2004/2005 Distinguished Research Professorship at the University of Western Ontario.

Observe that from basic properties of p-groups it follows that for each open subgroup H of G there exists a chain of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_k = H$$

such that G_{i+1} is normal in G_i and $[G_i : G_{i+1}] = p$ for each $i = 0, 1, \ldots, k-1$. Since closed subgroups of free pro-p-groups are free [S1, Corollary 3, §I.4.2], Schreier's formula (1) is equivalent to the seemingly weaker statement that the formula holds for all open subgroups H of G of index p:

$$h_1(H) = 1 + p(h_1(G) - 1). \tag{2}$$

We deduce a remarkable generalization of Schreier's formula for each $n \in \mathbb{N}$, as follows. Let $F^\times$ denote the nonzero elements of a field F, and for $c \in F^\times$, let $(c) \in H^1(G, \mathbb{F}_p)$ denote the corresponding class. For $\alpha \in H^m(G, \mathbb{F}_p)$ abbreviate by $\operatorname{ann}_n \alpha$ the annihilator

$$\operatorname{ann}_n \alpha = \{\beta \in H^n(G, \mathbb{F}_p) \mid \alpha \cup \beta = 0\}.$$

Finally, set $h_n(G) = \dim_{\mathbb{F}_p} H^n(G, \mathbb{F}_p)$.

Theorem 1. *Suppose that $\xi_p \in F$ and assume that F is perfect if $p > 2$. Suppose that $h_n(G) < \infty$. Let H be an open subgroup of G of index p, with fixed field $F(\sqrt[p]{a})$. Then*

$$h_n(H) = a_{n-1}(G, H) + p\big(h_n(G) - a_{n-1}(G, H)\big),$$

where $a_{n-1}(G, H)$ is the codimension of $\operatorname{ann}_{n-1}(a)$*:*

$$a_{n-1}(G, H) := \dim_{\mathbb{F}_p} \big(\ H^{n-1}(G, \mathbb{F}_p) / \operatorname{ann}_{n-1}(a) \ \big).$$

The proof of Theorem 1 brings additional insight into the structure of Schreier's formula; in fact, it makes Schreier's formula transparent for any $n \in \mathbb{N}$. In section 1, we derive several interpretations for the statement $\operatorname{cd}(G) = n$. First, we prove in Theorem 2 that if F contains a primitive pth root of unity ξ_p and F is perfect if $p > 2$, then $\operatorname{cd}(G) \le n$ if and only if the corestriction maps $\operatorname{cor} : H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ are surjective for all open subgroups H of G of index p. As a corollary, we show that the corresponding cohomology groups $H^{n+1}(H, \mathbb{F}_p)$ are all free as $\mathbb{F}_p[G/H]$-modules if and only if $\operatorname{cd}(G) \le n$, under the additional hypothesis that $F = F^2 + F^2$ when $p = 2$. Finally, we show in Theorem 3 that if G is finitely generated, then $\operatorname{cd}(G) \le n$ if and only if a single corestriction map, from the Frattini subgroup $\Phi(G) = G^p[G, G]$ of G, is surjective. In section 2 we prove Theorem 1.

For basic facts about Galois cohomology and maximal p-extensions of fields, we refer to [K] and [S1]. In particular, we work in the category of pro-p-groups.

1. When is $\mathrm{cd}(G) = n$?

As a consequence of recent results of Rost and Voevodsky on the Bloch-Kato conjecture, we have the following interesting translation of the statement $\mathrm{cd}(G) \leq n$ for a given $n \in \mathbb{N}$.

Theorem 2. *Suppose that $\xi_p \in F$ and assume that F is perfect if $p > 2$. Then for each $n \in \mathbb{N}$ we have $\mathrm{cd}(G) \leq n$ if and only if*

$$\mathrm{cor} : H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$$

is surjective for every open subgroup H of G of index p.

Proof. Suppose that F satisfies the conditions of the theorem, and let $G_{F(p)}$ be the absolute Galois group of $F(p)$.

Observe that since F contains ξ_p, the maximal p-extension $F(p)$ is closed under taking pth roots and hence $H^1(G_{F(p)}, \mathbb{F}_p) = \{0\}$. By the Bloch-Kato conjecture, proved in [V1, Theorem 7.1], the subring of the cohomology ring $H^\star(G_{F(p)}, \mathbb{F}_p)$ consisting of elements of positive degree is generated by cup-products of elements in $H^1(G_{F(p)}, \mathbb{F}_p)$. Hence $H^n(G_{F(p)}, \mathbb{F}_p) = \{0\}$ for $n \in \mathbb{N}$. Then, considering the Lyndon-Hochschild-Serre spectral sequence associated to the exact sequence

$$1 \to G_{F(p)} \to G_F \to G \to 1,$$

we have that

$$\mathrm{inf} : H^\star(G, \mathbb{F}_p) \to H^\star(G_F, \mathbb{F}_p) \tag{3}$$

is an isomorphism.

Now suppose that $\mathrm{cor} : H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective for all open subgroups H of G of index p. Let K be the fixed field of such a subgroup H. Then $K = F(\sqrt[p]{a})$ for some $a \in F^\times$. From Voevodsky's theorem [V1, Proposition 5.2], modified in [LMS1, Theorem 5] and translated to G from G_F via the inflation maps (3) above, we obtain the following exact sequence:

$$H^n(H, \mathbb{F}_p) \xrightarrow{\mathrm{cor}} H^n(G, \mathbb{F}_p) \xrightarrow{-\cup(a)} H^{n+1}(G, \mathbb{F}_p) \xrightarrow{\mathrm{res}} H^{n+1}(H, \mathbb{F}_p). \tag{4}$$

Therefore $\mathrm{res} : H^{n+1}(G, \mathbb{F}_p) \to H^{n+1}(H, \mathbb{F}_p)$ is injective for every open subgroup H of G of index p.

Now consider an arbitrary element

$$\alpha = (a_1) \cup \cdots \cup (a_{n+1}) \in H^{n+1}(G, \mathbb{F}_p),$$

where $a_i \in F^\times$ and (a_i) is the element of $H^1(G, \mathbb{F}_p)$ associated to a_i, $i = 1, 2, \ldots, n+1$. Suppose that $(a_1) \neq 0$, and set $K = F(\sqrt[p]{a_1})$ and $H = \mathrm{Gal}(F(p)/K)$. We have $0 = \mathrm{res}(\alpha) \in H^{n+1}(H, \mathbb{F}_p)$. Since res is injective, $\alpha = 0$. Again by the Bloch-Kato conjecture [V1, Theorem 7.1], we know that $H^{n+1}(G, \mathbb{F}_p)$ is generated by the elements α above. Hence $H^{n+1}(G, \mathbb{F}_p) = \{0\}$ and therefore $\mathrm{cd}(G) \leq n$. (See [K, page 49].)

Conversely, if $\mathrm{cd}(G) \leq n$ then from exact sequence (4) we conclude that $\mathrm{cor} : H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective for open subgroups H of G of index p. $\square$

Using conditions obtained in [LMS2] for $H^n(H, \mathbb{F}_p)$ to be a free $\mathbb{F}_p[G/H]$-module, we obtain the following corollary. We observe the convention that $\{0\}$ is a free $\mathbb{F}_p[G/H]$-module.

Corollary. *Suppose that $\xi_p \in F$ and assume that F is perfect if $p > 2$. If $p = 2$ assume also that $F = F^2 + F^2$. Then for each $n \in \mathbb{N}$, we have that $H^{n+1}(H, \mathbb{F}_p)$ is a free $\mathbb{F}_p[G/H]$-module for every open subgroup H of G of index p if and only if $\mathrm{cd}(G) \leq n$.*

Observe that the condition $F = F^2 + F^2$ is satisfied in particular when F contains a primitive fourth root of unity i: for all $c \in F^\times$, $c = ((c+1)/2)^2 + ((c-1)i/2)^2$.

Proof. Assume that F is as above, $n \in \mathbb{N}$, and that $H^{n+1}(H, \mathbb{F}_p)$ is a free $\mathbb{F}_p[G/H]$-module for every open subgroup H of G of index p. If $p > 2$, then it follows from [LMS2, Theorem 1] that the corestriction maps $\mathrm{cor} : H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ are surjective for all such subgroups H.

If $p = 2$, then we consider open subgroups H of index 2 with corresponding fixed fields $K = F(\sqrt{a})$. From [LMS2, Theorem 1] we obtain that $\mathrm{ann}_n(a) = \mathrm{ann}_n\big((a) \cup (-1)\big)$. It follows from the hypothesis $F = F^2 + F^2$ that $(c) \cup (-1) = 0 \in H^2(G, \mathbb{F}_2)$ for each $c \in F^\times$ and in particular for $c = a$. Hence $\mathrm{ann}_n(a) = H^n(G, \mathbb{F}_2)$. But then from exact sequence (4) above, we deduce that $\mathrm{cor} : H^n(H, \mathbb{F}_2) \to H^n(G, \mathbb{F}_2)$ is surjective.

Since our analysis holds for all open subgroups H of index p, by Theorem 2 we conclude that $\mathrm{cd}(G) \leq n$.

Assume now that $\mathrm{cd}(G) \leq n$. Then by Serre's theorem in [S2] we find that $\mathrm{cd}(H) \leq n$ for every open subgroup H of G. Hence $H^{n+1}(H, \mathbb{F}_p) = \{0\}$ which, by our convention, is a free $\mathbb{F}_p[G/H]$-module, as required. □

Remark. When $p = 2$ and $F \neq F^2 + F^2$, the statement of the corollary may fail. Consider the case $F = \mathbb{R}$. Then the only subgroup H of index 2 in $G = \mathbb{Z}/2\mathbb{Z}$ is $H = \{1\}$. Then for all $n \in \mathbb{N}$, $H^{n+1}(H, \mathbb{F}_2) = \{0\}$ and is free as an $\mathbb{F}_2[G/H]$-module. However, $\mathrm{cd}(G) = \infty$.

Under the additional assumption that G is finitely generated, we show that the surjectivity of a single corestriction map is equivalent to $\mathrm{cd}(G) \leq n$.

Theorem 3. *Suppose that $\xi_p \in F$ and assume that F is perfect if $p > 2$. Suppose that G is finitely generated. Then for each $n \in \mathbb{N}$ we have $\mathrm{cd}(G) \leq n$ if and only if*

$$\mathrm{cor} : H^n(\Phi(G), \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$$

is surjective.

Proof. Because G is finitely generated, the index $[G : \Phi(G)]$ is finite, and we may consider a suitable chain of open subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_k = \Phi(G)$$

such that $[G_i : G_{i+1}] = p$ for each $i = 0, 1, \ldots, k-1$.

By Serre's theorem in [S2], $\mathrm{cd}(H) = \mathrm{cd}(G)$ for every open subgroup H of G. Hence if $\mathrm{cd}(G) \leq n$ we may iteratively apply Theorem 2 to the chain of open subgroups to conclude that

$$\mathrm{cor} : H^n(\Phi(G), \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$$

is surjective.

Assume now that $\mathrm{cor} : H^n(\Phi(G), \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective. For each open subgroup H of G of index p we have a commutative diagram of corestriction maps

$$\begin{tikzcd} H^n(\Phi(G), \mathbb{F}_p) \arrow[r] \arrow[dr] & H^n(H, \mathbb{F}_p) \arrow[d] \\ & H^n(G, \mathbb{F}_p) \end{tikzcd}$$

since $\Phi(G) \subset H$. We obtain that $\operatorname{cor} : H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective, and by Theorem 2 we deduce that $\operatorname{cd}(G) \leq n$, as required. □

2. Schreier's Formula for H^n

We now prove Theorem 1. Suppose that $\operatorname{cd}(G) = n$, and let H be an open subgroup of G of index p. By Theorem 2, the corestriction map $\operatorname{cor} : H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective.

Let $K = F(\sqrt[p]{a})$ be the fixed field of H. Since $H^{n+1}(G, \mathbb{F}_p) = \{0\}$ by hypothesis, we conclude that $\operatorname{ann}_{n-1}\big((a) \cup (\xi_p)\big) = H^{n-1}(G, \mathbb{F}_p)$. Then by [LMS1, Theorem 1], we obtain the decomposition

$$H^n(H, \mathbb{F}_p) = X \oplus Y,$$

where X is a trivial $\mathbb{F}_p[G/H]$-module and Y is a free $\mathbb{F}_p[G/H]$-module. Moreover

$$x := \operatorname{rank}_{\mathbb{F}_p} X = \dim_{\mathbb{F}_p} H^{n-1}(G, \mathbb{F}_p)/\operatorname{ann}_{n-1}(a) = a_{n-1}(G, H), \quad \text{and}$$
$$y := \operatorname{rank}\ Y = \dim_{\mathbb{F}_p} H^n(G, \mathbb{F}_p)/(a) \cup H^{n-1}(G, \mathbb{F}_p).$$

Therefore $h_n(H) = \dim_{\mathbb{F}_p} H^n(H, \mathbb{F}_p) = x + py$.

Now, considering the exact sequence

$$0 \to \frac{H^{n-1}(G, \mathbb{F}_p)}{\operatorname{ann}_{n-1}(a)} \xrightarrow{-\cup(a)} H^n(G, \mathbb{F}_p) \to \frac{H^n(G, \mathbb{F}_p)}{(a) \cup H^{n-1}(G, \mathbb{F}_p)} \to 0,$$

we see that $\dim_{\mathbb{F}_p} H^n(H, \mathbb{F}_p)$ is equal to the sum of the dimension x of the kernel and p times the dimension y of the cokernel, and the theorem follows.

Observe that we have established a more general formula than the formula displayed in Theorem 1, since we have not assumed that $h_n(G)$ is finite.

When $n = 1$, $\operatorname{ann}_{n-1}(a) = \{0\}$ so that $a_{n-1}(G, H) = 1$. Therefore when G is finitely generated we recover Schreier's formula (2):

$$h_1(H) = 1 + p(h_1(G) - 1).$$

References

[K] H. Koch, *Galois theory of p-extensions*. Berlin: Springer-Verlag, 2002.

[LMS1] N. Lemire, J. Mináč, and J. Swallow. Galois module structure of Galois cohomology. ArXiv:math.NT/0409484 (2004).

[LMS2] N. Lemire, J. Mináč, and J. Swallow. When is Galois cohomology free or trivial? ArXiv:math.NT/0410617 (2004).

[S1] J.-P. Serre. *Galois cohomology.* Heidelberg: Springer-Verlag, 1997.

[S2] J.-P. Serre. Sur la dimension cohomologique des groupes profinis. *Topology* **3** (1965), 413–420.

[V1] V. Voevodsky. Motivic cohomology with $\mathbb{Z}/2$-coefficients. *Publ. Inst. Hautes Études Sci.*, No. 98 (2003), 59–104.

[V2] V. Voevodsky. On motivic cohomology with $\mathbb{Z}/l$ coefficients. K-theory preprint archive 639 (2003). www.math.uiuc.edu/K-theory/0639/.

Department of Mathematics and Statistics, McGill University, Burnside Hall, 805 Sherbrooke Street West, Montreal, Quebec H3A 2K6 CANADA

E-mail address: labute@math.mcgill.ca

Department of Mathematics, Middlesex College, University of Western Ontario, London, Ontario N6A 5B7 CANADA

E-mail address: nlemire@uwo.ca

E-mail address: minac@uwo.ca

Department of Mathematics, Davidson College, Box 7046, Davidson, North Carolina 28035-7046 USA

E-mail address: joswallow@davidson.edu