Canad. Math. Bull. Vol. **50** (4), 2007 pp. 588–593

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 p-th root of unity. Then for $n \in \mathbb{N}$, the cohomological dimension of the maximal pro-p-quotient G of the absolute Galois group of F is at most 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 generalize Schreier's formula for $\dim_{\mathbb{F}_p} H^1(H, \mathbb{F}_p)$ to $\dim_{\mathbb{F}_p} H^n(H, \mathbb{F}_p)$.

Introduction

For a prime p, let $F(p)$ denote the maximal p-extension of a field F. One of the fundamental problems 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].)

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:

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

Received by the editors May 12, 2005.

The research of the second author supported in part by NSERC grant R3276A0. The research of the third author 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.

AMS subject classification: 12G05, 12G10.

Keywords: cohomological dimension, Schreier's formula, Galois theory, p-extensions, pro-p-groups.

Using the Bloch–Kato conjecture (see [V1, V2, SJ]), we deduce a generalization of Schreier's formula for each $n \in \mathbb{N}$. The result requires a hypothesis on the surjectivity of a single corestriction map, from an open subgroup of index p, on degree n cohomology. By [NSW, Proposition 3.3.8], if $\operatorname{cd}(G) \leq n$, then this surjectivity of the corestriction holds for every open subgroup of G of index p. Conversely, in Section 1, we show that this surjectivity of the corestriction for every subgroup of index p implies $\operatorname{cd}(G) \leq n$. Hence the result generalizes Schreier's formula in two ways: first, from $n = 1$ to $n \in \mathbb{N}$, and second, from $\operatorname{cd}(G) = n$ to a condition on a single corestriction map.

Let ξ_p denote a p-th root of unity of order p, $F^\times$ 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. Moreover, $\alpha \in H^m(G, \mathbb{F}_p)$, 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 $h_n(G) < \infty$. Let H be an open subgroup of G of index p, with fixed field $F(\sqrt[p]{a})$, and suppose furthermore that the corestriction map $H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective. Then*

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

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

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

The proof of Theorem 1 provides additional insight into the structure of Schreier's formula; in fact, it makes Schreier's formula transparent from the Galois module point of view 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 p-th root of unity ξ_p, then $\operatorname{cd}(G) \leq n$ if and only if the corestriction maps $\operatorname{cor}\colon H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ 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 $\operatorname{cd}(G) \leq n$, under the additional hypothesis that $F = F^2 + F^2$ when $p = 2$. Finally, we show in Theorem 4 that if G is finitely generated, then $\operatorname{cd}(G) \leq n$ 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, S1]. In particular, we work in the category of pro-p-groups.

1 When Is $\operatorname{cd}(G) = n$?

From the Bloch–Kato conjecture [V1, V2, SJ], we have the following interesting translation of the statement $\operatorname{cd}(G) \leq n$ for a given $n \in \mathbb{N}$. Observe that when $\operatorname{cd}(G) \leq n$, the corestriction maps $\operatorname{cor}\colon H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ are surjective for all open subgroups H of G of index p [NSW, Proposition 3.3.8].

https://doi.org/10.4153/CMB-2007-056-3 Published online by Cambridge University Press

Theorem 2 *Suppose that $\xi_p \in F$. Then for each $n \in \mathbb{N}$ we have $\operatorname{cd}(G) \leq n$ if and only if $\operatorname{cor}\colon H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ 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 p-th roots, and hence $H^1(G_{F(p)}, \mathbb{F}_p) = \{0\}$. By the Bloch–Kato conjecture [V2, Theorem 7.1], the subring of the cohomology ring $H^*(G_{F(p)}, \mathbb{F}_p)$ 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 short exact sequence $1 \to G_{F(p)} \to G_F \to G \to 1$, we have that

$$\inf\colon H^*(G, \mathbb{F}_p) \to H^*(G_F, \mathbb{F}_p) \tag{3}$$

is an isomorphism.

Now suppose that $\operatorname{cor}\colon H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ 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 [V1, Lemma 6.11 and §7] and [V2, §6 and Theorem 7.1], as well as [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:

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

Therefore $\operatorname{res}\colon H^{n+1}(G, \mathbb{F}_p) \to H^{n+1}(H, \mathbb{F}_p)$ 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 $H = \operatorname{Gal}(F(p)/K)$. We have $0 = \operatorname{res}(\alpha) \in H^{n+1}(H, \mathbb{F}_p)$. 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 $\operatorname{cd}(G) \leq n$. (See [K, page 49].)

Conversely, if $\operatorname{cd}(G) \leq n$ then by [NSW, Proposition 3.3.8] we conclude that $\operatorname{cor}\colon H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective for open subgroups H of G of index p. ∎

From now on we will use without mention the fact from the proof above that $\inf\colon H^*(G, \mathbb{F}_p) \to H^*(G_F, \mathbb{F}_p)$ and $\inf\colon H^*(H, \mathbb{F}_p) \to H^*(G_K, \mathbb{F}_p)$ are isomorphisms, as well as the fact that the latter isomorphism is $\operatorname{Gal}(K/F)$-equivariant.

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 3 *Suppose that $\xi_p \in F$ and if $p = 2$; suppose 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 $\operatorname{cd}(G) \leq n$.*

https://doi.org/10.4153/CMB-2007-056-3 Published online by Cambridge University Press

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 $\mathrm{cor}\colon H^n(H, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ 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 $\mathrm{ann}_n(a) = \mathrm{ann}_n((a) \cup (-1))$. 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 $\mathrm{cor}\colon H^n(H, \mathbb{F}_2) \to H^n(G, \mathbb{F}_2)$ is surjective.

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

Assume now that $\mathrm{cd}(G) \le n$. Then by Serre's theorem in [S2] we find that $\mathrm{cd}(H) \le n$ 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 will show that the surjectivity of a single corestriction map is equivalent to $\mathrm{cd}(G) \le n$.

Theorem 4 *Suppose that $\xi_p \in F$ and G is finitely generated. Then for each $n \in \mathbb{N}$ we have* $\mathrm{cd}(G) \le n$ *if and only if* $\mathrm{cor}\colon H^n(\Phi(G), \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ *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 $i = 0, 1, \dots, k-1$. (Then each G_{i+1} is a normal subgroup of G_i.)

If $\mathrm{cd}(G) \le n$, then by Serre's theorem [S2], $\mathrm{cd}(H) = \mathrm{cd}(G)$ for every open subgroup H of G. Hence if $\mathrm{cd}(G) \le n$, we may iteratively apply Theorem 2 to the chain of open subgroups to conclude that $\mathrm{cor}\colon H^n(\Phi(G), \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective. (Alternatively, we could use [NSW, Proposition 3.3.8] to deduce that this corestriction map is surjective.)

Assume now that $\mathrm{cor}\colon H^n(\Phi(G), \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is surjective. For each open

https://doi.org/10.4153/CMB-2007-056-3 Published online by Cambridge University Press

subgroup H of G of index p we have a commutative diagram of corestriction maps

$$\begin{array}{ccc} H^n(\Phi(G),\mathbb{F}_p) & \longrightarrow & H^n(H,\mathbb{F}_p) \\ & \searrow & \downarrow \\ & & H^n(G,\mathbb{F}_p), \end{array}$$

since $\Phi(G) \subset H$. We obtain that $\operatorname{cor}\colon H^n(H,\mathbb{F}_p) \to H^n(G,\mathbb{F}_p)$ 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 H is an open subgroup of G of index p and the corestriction map $\operatorname{cor}\colon H^n(H,\mathbb{F}_p) \to H^n(G,\mathbb{F}_p)$ is surjective. Let $K = F(\sqrt[p]{a})$ be the fixed field of H.

We claim that $\operatorname{ann}_{n-1}((a)\cup(\xi_p)) = H^{n-1}(G,\mathbb{F}_p)$. Suppose that $\alpha \in H^{n-1}(G,\mathbb{F}_p)$. By the surjectivity hypothesis there exists $\beta \in H^n(H,\mathbb{F}_p)$ such that $\operatorname{cor}\beta = (\xi_p)\cup\alpha$. From [V1, Proposition 5.2] modified in [LMS1, Theorem 5], $(a) \cup (\operatorname{cor}\ \beta) = 0$ and hence $(a)\cup(\xi_p)\cup\alpha = 0$. Therefore the claim is established. 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. (Because $\operatorname{ann}_{n-1}((a)\cup(\xi_p)) = H^{n-1}(G,\mathbb{F}_p)$, there are no 2-dimensional summands when $p > 2$, and by the surjectivity of the corestriction map, the summand Z in [LMS1, Theorems 1 and 2], a trivial $\mathbb{F}_p[G/H]$-module, is also $\{0\}$.) Moreover, from [LMS1, Theorems 1 and 2] we have

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

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 our formula $h_n(H) = x + py$ holds without the assumption that $h_n(G)$ is finite. (This assumption is used only in the formulation of Theorem 1 where we subtract $a_{n-1}(G,H)$ from $h_n(G)$.)

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*. Translated from the 1970 German original by Franz Lemmermeyer. With a postscript by the author and Lemmermeyer. Springer-Verlag, Berlin, 2002.

[LMS1] N. Lemire, J. Mináč, and J. Swallow, *Galois module structure of Galois cohomology and partial Euler-Poincaré characteristics.*To appear in J. Reine Angew. Math. ArXiv:math.NT/0409484, 2004.

[LMS2] ———, *When is Galois cohomology free or trivial?* New York J. Math. **11**(2005), 291–302.

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields.* Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, Berlin, 2000.

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

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

[SJ] A. Suslin and S. Joukhovitski, *Norm varieties.* J. Pure Appl. Algebra **206**(2006), no. 1-2, 245–276.

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

[V2] ———, *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
805 Sherbrooke Street West
Montreal, QC
H3A 2K6
e-mail: labute@math.mcgill.ca

Department of Mathematics
Middlesex College
University of Western Ontario
London, ON
N6A 5B7
e-mail: nlemire@uwo.ca
minac@uwo.ca

Department of Mathematics
Davidson College
Davidson, NC 28035-7046
U.S.A.
e-mail: joswallow@davidson.edu