DEMUŠKIN GROUPS, GALOIS MODULES, AND THE ELEMENTARY TYPE CONJECTURE

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

ABSTRACT. Let p be a prime and $F(p)$ the maximal p-extension of a field F containing a primitive p-th root of unity. We give a new characterization of Demuškin groups among Galois groups $\mathrm{Gal}(F(p)/F)$ when $p = 2$, and, assuming the Elementary Type Conjecture, when $p > 2$ as well. This characterization is in terms of the structure, as Galois modules, of the Galois cohomology of index p subgroups of $\mathrm{Gal}(F(p)/F)$.

Let p be a prime and F a field containing a primitive p-th root of unity ξ_p. The union $F(p)$ of all finite Galois extensions L/F in a fixed algebraic closure of F with $[L : F]$ a power of p is called the maximal p-extension of F. Consider $G = \mathrm{Gal}(F(p)/F)$. Observe that while every profinite group is a Galois group of some Galois extension [W1], the condition that $G = \mathrm{Gal}(F(p)/F)$ is substantially more restrictive.

We ask when $G = \mathrm{Gal}(F(p)/F)$ is a Demuškin group, that is, a finitely generated pro-p-group satisfying $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$ such that the cup product

$$\gamma_F : H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$$

is a nondegenerate bilinear form. (See [NSW, §III.9] and [S, §I.4.5 and §II.5.6]. Others relax the requirement on finite generation, but in this article we consider only the finitely generated case.) Demuškin groups arise, for instance, as pro-p-completions of fundamental groups of compact surfaces T of genus $g \geq 1$ when T is orientable and $g \geq 2$ when T is not orientable. If F is a finite extension of the field of p-adic numbers $\mathbb{Q}_p$ and contains ξ_p, then G is Demuškin.

Date: December 12, 2005.

†Research supported in part by NSERC grant R3276A01.

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

The study of Demuškin groups among Galois groups $\mathrm{Gal}(F(p)/F)$ is an important part of the program of classification of possible Galois groups of maximal p-extensions of fields, as these groups form an essential part of the local theory of this project. In turn, the classification of possible $\mathrm{Gal}(F(p)/F)$ is one of the key problems in current Galois theory. This study is also crucial for the development of anabelian algebraic geometry over fields. (See [Ef3], [Ko], and further references in these papers.)

In this paper we detect whether $G = \mathrm{Gal}(F(p)/F)$ is a Demuškin group in terms of the Galois module structure of the Galois cohomology of index p subgroups of G. For such G, we establish a new characterization of Demuškin groups when $p = 2$. When $p > 2$ our characterization depends upon the Elementary Type Conjecture in the theory of Galois pro-p-groups. The close relationship of this characterization with the Elementary Type Conjecture offers a new approach to the Conjecture. (See Remark 2 in section 5.)

The surprising new insight contained in Theorem 1 below is that G is Demuškin if $\mathrm{cd}(G) = 2$ and $H^2(N, \mathbb{F}_p)$, with N a subgroup of index p of G, does not grow "too fast." In fact a relatively mild condition on the growth of $H^2(N, \mathbb{F}_p)$ guarantees that $\dim_{\mathbb{F}_p} H^2(N, \mathbb{F}_p) = 1$.

In considering Galois cohomology groups as Galois modules, we could use the results of [LMS1] and [LMS2]. These results, however, depend upon recent, complex, partially published work of Rost-Voevodsky on the Bloch-Kato Conjecture. For the proof of the following theorem we use only the results in [MeSu] concerning the Bloch-Kato Conjecture in the case $n = 2$.

Before formulating the main theorem we recall that if G is a finitely generated pro-p-group, any subgroup of index p is closed [S, §I.4.2, Ex. 6], and that in a pro-p-group, any subgroup of index p is normal. Let H be a group and M be an $\mathbb{F}_p[H]$-module. We say that M is a trivial $\mathbb{F}_p[H]$-module if for each $\tau \in H$ and $m \in M$ we have $\tau(m) = m$.

Theorem 1. *Let F be a field containing a primitive p-th root of unity, and suppose that $G = \mathrm{Gal}(F(p)/F)$ is a finitely generated pro-p-group of cohomological dimension 2. Then for each subgroup N of G of index p, the following conditions on the $\mathbb{F}_p[G/N]$-module $H^2(N, \mathbb{F}_p)$ are equivalent:*

(1) *$H^2(N, \mathbb{F}_p)$ has no nonzero free summand.*
(2) *$H^2(N, \mathbb{F}_p)$ is a trivial $\mathbb{F}_p[G/N]$-module.*

Now assume additionally that either $p = 2$ or $p > 2$ and the Elementary Type Conjecture holds. (See the end of section 2.)

Then G is Demuškin if and only if, for every subgroup N of G of index p, $H^2(N, \mathbb{F}_p)$ has no nonzero free summand.

We observe that the Elementary Type Conjecture has been established for some important classes of fields, including algebraic extensions F of $\mathbb{Q}$ with finitely generated $G = \mathrm{Gal}(F(p)/F)$. (See [Ef1] and [Ef2].) For such fields Theorem 1 is a precise characterization. For additional information about the Elementary Type Conjecture see [Ma2].

In [DuLa, Theorem 1] it was shown that a finitely generated pro-p-group G such that $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) > 1$ and $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$ is Demuškin if and only if $H^2(N, \mathbb{F}_p) \cong \mathbb{F}_p$ for all subgroups N of G of index p. Note that in Theorem 1, under the assumption that $\mathrm{cd}(G) = 2$ and, if $p > 2$, that the Elementary Type Conjecture holds, we do not require that $H^2(N, \mathbb{F}_p) \cong \mathbb{F}_p$ but instead only that $H^2(N, \mathbb{F}_p)$ contains no nonzero free summand. In fact, we prove more than we claim in Theorem 1. Namely, from the proof of Theorem 1 it follows that we can replace the hypothesis $\mathrm{cd}(G) = 2$ by two conditions which follow from it: first, that the corestriction map from $H^2(N, \mathbb{F}_p)$ to $H^2(G, \mathbb{F}_p)$ is surjective for all subgroups N of G of index p, and, second, that $H^2(G, \mathbb{F}_p)$ is not zero. We use deep results from Galois cohomology in our proof, and it would be interesting to see whether these characterizations of Demuškin groups among groups $\mathrm{Gal}(F(p)/F)$ also hold in the category of pro-p-groups.

The heart of our analysis is section 4, where we determine the structure of the $\mathbb{F}_p[G/N]$-module $H^2(N, \mathbb{F}_p)$ when N is a subgroup of G of index p and the corestriction map $\mathrm{cor} : H^2(N, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is surjective. In particular, we show that $H^2(N, \mathbb{F}_p) \cong X \oplus Y$ where X is trivial and Y is a free $\mathbb{F}_p[G/N]$-module. Moreover, we characterize all such decompositions of $H^2(N, \mathbb{F}_p)$. We believe that these results are of independent interest; for example, we obtain immediately from this structure some information on the size of $H^2(N, \mathbb{F}_p)$. (See the Corollary to Theorem 3.)

Our approach uses p-quaternionic pairings, and we closely follow [Ku2] in the first two sections. Some of the basic concepts recalled here were introduced by Hwang and Jacob in [HJ]. In the next sections we consider $H^2(G, \mathbb{F}_2)$ when cup products are strongly regular, as well as the Galois module structure of $H^2(N,\mathbb{F}_p)$ for index p subgroups N of G when the corestriction is surjective. Then we prove Theorem 1 and its Corollary. Finally, we close with a consideration of the $\mathbb{F}_p[G/N]$-module structure of the 1-cohomology groups $H^1(N,\mathbb{F}_p)$.

1. p-Quaternionic Pairings

We seek to understand the condition on the cup product in the definition of Demuškin groups by considering such products in the context of p-quaternionic pairings and bilinear forms in general.

Let H and Q be elementary abelian p-groups written multiplicatively and additively, respectively, and if $p=2$ choose a distinguished element $-1\in H$, which may be trivial. Let $\gamma : H\times H\to Q$ be a bilinear form. For a given element $a\in H$, we define the group homomorphism

$$\gamma_a : H\to Q,\qquad \gamma_a(x) := \gamma(a,x),\quad x\in H,$$

and we denote by $Q(a)$ the value group $\gamma_a(H)$ of γ_a. We also define

$$N(a)=N_\gamma(a)=\ker\gamma_a=\{b\in H \ \mid\ \gamma(a,b)=0\}\,.$$

We have $H/N(a)\cong Q(a)$.

The bilinear form γ is called *nondegenerate* if $Q(a)\neq\{0\}$ for all $a\in H\setminus\{1\}$. If $Q(a)=Q$ for all $a\in H\setminus\{1\}$, then the bilinear mapping γ is called *strongly regular*.

Observe that in the following definition of p-quaternionic pairing, the distinguished involution $-1\in H$ is necessarily 1 if $p>2$.

We say that (H,Q,γ) is a *p-quaternionic pairing* if there exists a distinguished involution $-1\in H$ such that:

(1) Q is generated by the union $\bigcup_{a\in H}Q(a)$ of the value groups;
(2) $\gamma(a,a)=\gamma(a,-1)$ for all $a\in H$;
(3) if $p=2$ then γ satisfies *the linkage condition*: if for $a,b,c,d\in H$ we have that $\gamma(a,b)=\gamma(c,d)$, then there exists $e\in H$ such that

$$\gamma(a,b)=\gamma(a,e)=\gamma(c,e)=\gamma(c,d);$$

and

(4) for every $n \geq 2$, the $M(n)$ *condition* holds: if for elements $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ of H with $a_1, \ldots, a_n$ linearly independent over $\mathbb{F}_p$, we have

$$\sum_{i=1}^{n} \gamma(a_i, b_i) = 0,$$

then there exist elements $a_{n+1}, \ldots, a_k \in H$, with $a_1, a_2, \ldots, a_k$ linearly independent over $\mathbb{F}_p$ and $x_{j_1,\ldots,j_k} \in N_\gamma\left(a_1^{j_1} a_2^{j_2} \cdots a_k^{j_k}\right)$ such that

$$b_i = \prod_{0 \leq j_1, j_2, \ldots, j_k \leq p-1} (x_{j_1,\ldots,j_k})^{j_i}, \quad i = 1, \ldots, k,$$

where $b_{n+1}, \ldots, b_k = 1$.

(It is worth observing that from the bilinearity of γ and condition (2), it follows that γ is skew-symmetric if $p > 2$ and symmetric if $p = 2$.)

A p-quaternionic pairing (H, Q, γ) is said to be *strongly regular* if γ is strongly regular. A p-quaternionic pairing is said to be *finite* if H is finite.

We consider several types of p-quaternionic pairings.

The cup product γ_F of a field F. Let F denote a field containing ξ_p and let $G = \mathrm{Gal}(F(p)/F)$. The cup product pairing

$$\gamma_F : H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$$

satisfies the $M(n)$ conditions (see [Me, Proposition 4] and [MeSu, (11.5) Theorem]). In fact, the $M(n)$ conditions are a translation of the condition for the splitting of a sum of n symbols in Milnor's $k_2F = K_2F/pK_2F$ to the language of p-quaternionic pairings. Observe that in [Ku2] the set of conditions $M(n), n \geq 2$, is a different condition than our condition (4), but the alteration of axiom (3) in [Ku2, p. 40] does not affect the results from [Ku2] that we use. Condition (1) also follows from [MeSu, (11.5) Theorem]. Condition (2) is true when the distinguished involution $(-1) \in H^1(G, \mathbb{F}_p)$ corresponds to $[-1] \in F^\times/F^{\times p}$ via Kummer theory. The linkage condition in (3) is well-known. (See [L, Chapter 3, Theorem 4.13].)

Pairings of p-local type. A finite p-quaternionic pairing (H, Q, γ) with Q a group of order p and γ nondegenerate is said to be *of p-local type.* If $G = \mathrm{Gal}(F(p)/F)$ is a Demuškin group, then it follows from the definition that $(H^1(G, \mathbb{F}_p), H^2(G, \mathbb{F}_p), \gamma_F)$ is a p-quaternionic pairing of p-local type.

Strongly regular pairings. Suppose that $(H, \mathbb{F}_p, \gamma)$ is a p-quaternionic non-degenerate pairing. Observe that for each $a \in H \setminus \{1\}$, the subgroup $N(a)$ of H is of index p. Moreover, for $a, b \in H \setminus \{1\}$ we have

$$N(a)N(b) \neq H \Longleftrightarrow N(a) = N(b) \Longleftrightarrow \langle a \rangle = \langle b \rangle.$$

Hence such p-quaternionic pairings are strongly regular. Now suppose instead that $Q = \{0\}$. If we set $\gamma(a, b) = 0$ for all $a, b \in H$, then (H, Q, γ) is a p-quaternionic pairing, called *totally degenerate*. Totally degenerate pairings are also strongly regular.

Pairings of weakly p-local type. A p-quaternionic pairing with $H = \{1\}$ is called *trivial*. Each trivial pairing is totally degenerate. We say that totally degenerate p-quaternionic pairings, as well as pairings of p-local type, are pairings *of weakly p-local type*.

2. p-Quaternionic Pairings and the Elementary Type Conjecture

For $p > 2$ we define the direct product and the group extension of p-quaternionic pairings and consider the Elementary Type Conjecture. Because we do not need it in Theorem 1, we do not consider the Elementary Type Conjecture when $p = 2$. (See [Ma1, Chap. 5] for the $p = 2$ case in the context of abstract Witt rings.)

(A) *Direct product.* Let (H_i, Q_i, γ_i), $i = 1, 2$, be p-quaternionic pairings. Define $H = H_1 \times H_2$, $Q = Q_1 \times Q_2$, and

$$\gamma\big([a_1, a_2], [b_1, b_2]\big) = \big[\gamma_1(a_1, b_1), \gamma_2(a_2, b_2)\big], \quad a_i, b_i \in H_i.$$

Then (H, Q, γ) is a p-quaternionic pairing called the *direct product*.

(B) *Group extension.* Suppose that (H', Q', γ') is a p-quaternionic pairing and let T be a nontrivial finite elementary abelian p-group. The *group extension* of (H', Q', γ') by T is the p-quaternionic pairing (H, Q, γ), where $H = H' \times T$, $Q = Q' \times (H' \otimes T) \times (T \wedge T)$, and the pairing $\gamma : H \times H \to Q$ is given by

$$\gamma\big([a_1, t_1], [a_2, t_2]\big) = \big[\gamma'(a_1, a_2), \quad a_1 \otimes t_2 - a_2 \otimes t_1, \quad t_1 \wedge t_2\big].$$

Here $\otimes$ denotes the tensor product over $\mathbb{F}_p$ and $\wedge$ the exterior product.

For $p > 2$, we say a that a finite p-quaternionic pairing is *of elementary type* if it may be constructed from p-quaternionic pairings of weakly p-local type using the operations of (a) direct product and

(b) group extension by nontrivial elementary abelian p-groups. The Elementary Type Conjecture for $p > 2$ is then as follows. (We note that there are several variants of the Elementary Type Conjecture which aim at the classification of finitely generated $\mathrm{Gal}(F(p)/F)$, contained in [Ef1], [Ef2], [En], [JW], and [Ma1, p. 123].)

Elementary Type Conjecture for Odd p. *Let $p > 2$ be a prime and F a field containing a primitive p-th root of unity. Suppose that $G = \mathrm{Gal}(F(p)/F)$ is a finitely generated pro-p-group. Then the cup product pairing γ_F is of elementary type.*

Theorem 2 ([Ku2, Corollary 5])**.** *For $p > 2$, a p-quaternionic pairing of elementary type is not strongly regular unless it is of weakly p-local type.*

3. Strongly regular cup products and $H^2(G, \mathbb{F}_2)$

For the proof of the following proposition we originally used streamlined arguments from [FY, pp. 42–43]. Afterwards Kula sent us a nice simplification of the proof, using ideas in [Ku1, Proof of Proposition 2.16]. We are grateful to him for permitting us to adapt this simplification for use here.

Proposition 1. *Let F be a field of characteristic not 2, and suppose that $G = \mathrm{Gal}(F(2)/F) \neq \{1\}$ is a finitely generated pro-2-group with γ_F nondegenerate and strongly regular. Then $H^2(G, \mathbb{F}_2) \cong \mathbb{F}_2$.*

Proof. Assume that the hypotheses of our proposition are valid, and denote by $|A|$ the cardinality of a set A. Because the statement is trivial in the case $|H^1(G, \mathbb{F}_2)| = 2$, we assume without loss of generality that $g := |H^1(G, \mathbb{F}_2)| > 2$. Denote $h := |H^2(G, \mathbb{F}_2)| > 1$, as γ_F is nondegenerate. Set $\mathrm{ann}(a) = \{(b) \in H^1(G, \mathbb{F}_2) \mid (a) \cdot (b) = 0\}$. Since $(a) \cdot H^1(G, \mathbb{F}_2) \cong H^1(G, \mathbb{F}_2)/\mathrm{ann}(a)$, we see that

$$|\mathrm{ann}(a)| = \frac{|H^1(G, \mathbb{F}_2)|}{|(a) \cdot H^1(G, \mathbb{F}_2)|} = \frac{|H^1(G, \mathbb{F}_2)|}{|H^2(G, \mathbb{F}_2)|} = \frac{g}{h}$$

for all nonzero $(a) \in H^1(G, \mathbb{F}_2)$.

We show now that for arbitrary distinct, nonzero elements $(a), (b) \in H^1(G, \mathbb{F}_2)$, we have $\mathrm{ann}(a) + \mathrm{ann}(b) = H^1(G, \mathbb{F}_2)$. Let $(x) \in H^1(G, \mathbb{F}_2)$ be arbitrary. If $q := (x) \cdot (a) = 0$, then $(x) \in \mathrm{ann}(a)$. Assume therefore that $q \neq 0$. Using the surjectivity of the map $((a) + (b)) \cdot - :$

$H^1(G,\mathbb{F}_2) \to H^2(G,\mathbb{F}_2)$ and the linkage property, we see that there exists $(c) \in H^1(G,\mathbb{F}_2)$ such that

$$q = (a)\cdot(x) = (a)\cdot(c) = ((a)+(b))\cdot(c).$$

Hence $((x)+(c))\cdot(a) = 0 = (b)\cdot(c)$ and therefore $(x)+(c) \in \operatorname{ann}(a)$ and $(c) \in \operatorname{ann}(b)$. Thus $(x) = ((x)+(c))+(c) \in \operatorname{ann}(a)+\operatorname{ann}(b)$, as required.

Let D be the set of nonzero elements in the dual space of $H^1(G,\mathbb{F}_2)$. Similarly, for each nonzero element $(a) \in H^1(G,\mathbb{F}_2)$, let $D_{(a)}$ be the set of all maps in D which are zero on $\operatorname{ann}(a)$. Because $\operatorname{ann}(a)+\operatorname{ann}(b) = H^1(G,\mathbb{F}_2)$ for all pairs of distinct, nonzero elements (a) and (b), D contains the disjoint union of all $D_{(a)}$ in D. Since $|D| = g-1$ and $|D_{(a)}| = h-1$ for each nonzero (a), we obtain $(g-1)(h-1) \le (g-1)$. Therefore $h = 2$. $\square$

4. Surjective Corestrictions and $H^2(N,\mathbb{F}_p)$

In the following theorem we do not assume that G is finitely generated.

Theorem 3. *Let F be a field containing a primitive p-th root of unity, and suppose that $G = \operatorname{Gal}(F(p)/F)$. Let N be a subgroup of G of index p, and suppose that the corestriction map $\operatorname{cor} : H^2(N,\mathbb{F}_p) \to H^2(G,\mathbb{F}_p)$ is surjective. Let $a \in F^\times$ be chosen so that the fixed field of N is $F(\sqrt[p]{a})$. Then the $\mathbb{F}_p[G/N]$-module $H^2(N,\mathbb{F}_p)$ decomposes as*

$$H^2(N,\mathbb{F}_p) = X \oplus Y$$

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

(1) $\dim_{\mathbb{F}_p} X = \dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p)/\operatorname{ann}(a)$
(2) $\operatorname{rank}_{\mathbb{F}_p[G/N]} Y = \dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p)/(a)\cdot H^1(G,\mathbb{F}_p)$.

After the proof, we characterize in Theorem 4 all decompositions of $H^2(N,\mathbb{F}_p)$ into direct sums of trivial and free submodules.

Observe that we have a natural sequence

$$0 \to H^1(G,\mathbb{F}_p)/\operatorname{ann}(a) \to H^2(G,\mathbb{F}_p) \to H^2(G,\mathbb{F}_p)/(a)\cdot H^1(G,\mathbb{F}_p) \to 0.$$

Assume that $d = \dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p) < \infty$, and set

$$x = \dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p)/\operatorname{ann}(a), \quad y = \dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p)/(a)\cdot H^1(G,\mathbb{F}_p).$$

Then $d = x + y$ and we have the following corollary on the size of $H^2(N,\mathbb{F}_p)$:

Corollary. *Assume that G and N are as above. Then*

$$\dim_{\mathbb{F}_p} H^2(N,\mathbb{F}_p) = x + py.$$

Before the proof we need several intermediate results. We assume throughout this section that F is a field containing a primitive p-th root of unity ξ_p, $G = \mathrm{Gal}(F(p)/F)$, N is a subgroup of G of index p with fixed field $K = F(\sqrt[p]{a})$, and σ denotes a fixed generator of G/N with $\sqrt[p]{a}^{\sigma-1} = \xi_p$. For a field F, let G_F denote its absolute Galois group. Observe that because $1+\sigma+\cdots+\sigma^{p-1} \equiv (\sigma-1)^{p-1}$ modulo p, the endomorphism $(\sigma-1)^{p-1}$ on $H^i(N,\mathbb{F}_p)$ is identical to the composition $\mathrm{res}\circ\mathrm{cor}$.

Proposition 2.

(1) *The inflation maps* $\inf : H^i(G,\mathbb{F}_p) \to H^i(G_F,\mathbb{F}_p)$ *and* $\inf : H^i(N,\mathbb{F}_p) \to H^i(G_K,\mathbb{F}_p)$, *$i = 1,2$, are isomorphisms. Moreover, the latter isomorphisms are $\mathbb{F}_p[G/N]$-equivariant.*
(2) *The kernel of the corestriction map* $\mathrm{cor} : H^2(N,\mathbb{F}_p) \to H^2(G,\mathbb{F}_p)$ *is $(\sigma-1)H^2(N,\mathbb{F}_p) + \mathrm{res}\, H^2(G,\mathbb{F}_p)$.*
(3) *The kernel of the restriction map* $\mathrm{res} : H^2(G,\mathbb{F}_p) \to H^2(N,\mathbb{F}_p)$ *is $(a)\cdot H^1(G,\mathbb{F}_p)$.*

Proof. (1). We prove first the statements for G and G_F. Observe that since F contains a primitive p-th root of unity, $F(p)$ is closed under taking p-th roots and hence $H^1(G_{F(p)},\mathbb{F}_p) = \{0\}$. Therefore by [MeSu, Theorem 11.5] we see that $H^2(G_{F(p)},\mathbb{F}_p) = \{0\}$ as well. Then, considering the Lyndon-Hochschild-Serre spectral sequence associated to $1 \to G_{F(p)} \to G_F \to G \to 1$, we obtain that $\inf : H^i(G,\mathbb{F}_p) \to H^i(G_F,\mathbb{F}_p)$ is an isomorphism for each $i = 1,2$. The proof that $\inf : H^i(N,\mathbb{F}_p) \to H^i(G_K,\mathbb{F}_p)$, $i = 1,2$ are isomorphisms follows as above. The fact that these isomorphisms are $\mathbb{F}_p[G/N]$-equivariant follows immediately from the explicit action of $\mathbb{F}_p[G/N]$ on cochains.

(2). By [MeSu, Proposition 15.1], the kernel of the corestriction map $\mathrm{cor} : H^2(G_K,\mathbb{F}_p) \to H^2(G_F,\mathbb{F}_p)$ is $(\sigma-1)H^2(G_K,\mathbb{F}_p) + \mathrm{res}\, H^2(G_F,\mathbb{F}_p)$. Hence the second row is exact in the following commutative diagram. (Observe that σ commutes with inf by (1), and the right-hand square commutes by [NSW, Proposition 1.5.5ii].)

$$\begin{tikzcd}
H^2(N,\mathbb{F}_p)\oplus H^2(G,\mathbb{F}_p) \arrow[r, "{(\sigma-1) \atop \oplus\,\mathrm{res}}"] \arrow[d, "\inf\oplus\inf"] & H^2(N,\mathbb{F}_p) \arrow[r, "\mathrm{cor}"] \arrow[d, "\inf"] & H^2(G,\mathbb{F}_p) \arrow[d, "\inf"] \\
H^2(G_K,\mathbb{F}_p)\oplus H^2(G_F,\mathbb{F}_p) \arrow[r, "{(\sigma-1) \atop \oplus\,\mathrm{res}}"] & H^2(G_K,\mathbb{F}_p) \arrow[r, "\mathrm{cor}"] & H^2(G_F,\mathbb{F}_p)
\end{tikzcd}$$

The first row is therefore exact and we have our statement.

(3). By [Me, Proposition 5] and [MeSu, Theorem 11.5], the kernel of the restriction map $\mathrm{res} : H^2(G_F,\mathbb{F}_p) \to H^2(G_K,\mathbb{F}_p)$ is $(a)\cdot H^1(G_F,\mathbb{F}_p)$. A commutative diagram analogous to that of part (2) then gives our statement. ☐

Corollary. *Suppose that the corestriction map* $\mathrm{cor} : H^2(N,\mathbb{F}_p) \to H^2(G,\mathbb{F}_p)$ *is surjective. Then* $\ker \mathrm{cor} = (\sigma-1)H^2(N,\mathbb{F}_p)$.

Proof. By part (2) above, it is sufficient to show that $\mathrm{res}\, H^2(G,\mathbb{F}_p)$ is a subset of $(\sigma-1)H^2(N,\mathbb{F}_p)$. Let $\alpha \in H^2(G,\mathbb{F}_p)$. By hypothesis, there exists $\beta \in H^2(N,\mathbb{F}_p)$ such that $\mathrm{cor}\,\beta = \alpha$. Recalling that $\mathrm{res}\,\mathrm{cor} = (\sigma-1)^{p-1}$, we see that $\mathrm{res}\,\alpha = (\sigma-1)^{p-1}\beta \in (\sigma-1)H^2(N,\mathbb{F}_p)$. ☐

Lemma 1. *Suppose that the corestriction map* $\mathrm{cor} : H^2(N,\mathbb{F}_p) \to H^2(G,\mathbb{F}_p)$ *is surjective. Then there exists a trivial* $\mathbb{F}_p[G/N]$*-submodule* X *of* $H^2(N,\mathbb{F}_p)$ *such that*

$$\mathrm{cor} : X \to (a)\cdot H^1(G,\mathbb{F}_p)$$

is an isomorphism. In fact, $\mathrm{cor}(H^2(N,\mathbb{F}_p)^{G/N}) = (a)\cdot H^1(G,\mathbb{F}_p)$.

Proof. Let $\mathcal{I}$ be an $\mathbb{F}_p$-basis for $(a)\cdot H^1(G,\mathbb{F}_p) \subset H^2(G,\mathbb{F}_p)$. For each $(a)\cdot(f) \in \mathcal{I}$ we will define an element $x_f \in H^2(N,\mathbb{F}_p)$ such that $\mathrm{cor}\, x_f = (a)\cdot(f)$ and $(\sigma-1)x_f = 0$. Then the $\mathbb{F}_p$-span X of x_f will be our required module X. If $p = 2$, then we proceed as follows. By hypothesis there exists $x_f \in H^2(N,\mathbb{F}_2)$ such that $\mathrm{cor}\, x_f = (a)\cdot(f)$. Then

$$(\sigma-1)x_f = (\sigma+1)x_f = \mathrm{res}\,\mathrm{cor}\, x_f = \mathrm{res}((a)\cdot(f)) = 0,$$

and hence $x_f \in H^2(N,\mathbb{F}_2)^{G/N}$.

Now suppose that $p > 2$. If $\mathrm{res}((\xi_p)\cdot(f)) = 0$ then set $x_f = (\sqrt[p]{a})\cdot(f)$. Observe that in this case $x_f \in H^2(N,\mathbb{F}_p)^{G/N}$ and by the projection formula [NSW, Proposition 1.5.3iv], we have $\mathrm{cor}\, x_f = (a)\cdot(f)$. Otherwise, by hypothesis there exists $\alpha \in H^2(N,\mathbb{F}_p)$ such that $\mathrm{cor}\,\alpha = (\xi_p)\cdot(f)$.

Let $\beta = (\sigma-1)^{p-2}\alpha$. From $(\sigma-1)^{p-1} = \operatorname{res}\operatorname{cor}$ we obtain $(\sigma-1)\beta = \operatorname{res}((\xi_p)\cdot(f))$. Now set $x_f := (\sqrt[p]{a})\cdot(f) - \beta$. Then

$$(\sigma-1)x_f = \operatorname{res}((\xi_p)\cdot(f)) - \operatorname{res}((\xi_p)\cdot(f)) = 0,$$

so $x_f \in H^2(N,\mathbb{F}_p)^{G/N}$. Observe that since the corestriction commutes with σ [NSW, Proposition 1.5.4], cor vanishes on the image of $\sigma - 1$. Hence $\operatorname{cor}\beta = 0$. By the projection formula again, $\operatorname{cor} x_f = (a)\cdot(f)$.

Letting X be the $\mathbb{F}_p$-span of the elements x_f, we have the first statement of the lemma.

For the second statement, let $\gamma \in H^2(N,\mathbb{F}_p)^{G/N}$. Then $\operatorname{res}\operatorname{cor}\gamma = (\sigma-1)^{p-1}\gamma = 0$. By Proposition 2, part (3),

$$\operatorname{cor}\gamma \in \ker\operatorname{res} = (a)\cdot H^1(G,\mathbb{F}_p).$$

Therefore $\operatorname{cor}(H^2(N,\mathbb{F}_p)^{G/N}) \subset (a)\cdot H^1(G,\mathbb{F}_p)$. The reverse inclusion follows from the first statement. □

Lemma 2. *Suppose that the corestriction map* cor : $H^2(N,\mathbb{F}_p) \to H^2(G,\mathbb{F}_p)$ *is surjective. Then*

$$H^2(N,\mathbb{F}_p)^{G/N} \cap (\sigma-1)H^2(N,\mathbb{F}_p) = (\sigma-1)^{p-1}H^2(N,\mathbb{F}_p).$$

Proof. Since

$$(\sigma-1)^{p-1}H^2(N,\mathbb{F}_p) \subset H^2(N,\mathbb{F}_p)^{G/N} \cap (\sigma-1)H^2(N,\mathbb{F}_p),$$

it is sufficient to prove the reverse inclusion. If $p = 2$ the reverse inclusion is true since $(\sigma-1)H^2(N,\mathbb{F}_p) \subset H^2(N,\mathbb{F}_p)^{G/N}$. Therefore assume that $p > 2$.

Let

$$\gamma \in H^2(N,\mathbb{F}_p)^{G/N} \cap (\sigma-1)H^2(N,\mathbb{F}_p).$$

Since $0 \in (\sigma-1)^{p-1}H^2(N,\mathbb{F}_p)$ we also assume that $\gamma \neq 0$. Then $\gamma = (\sigma-1)\beta$ for some $\beta \in H^2(N,\mathbb{F}_p)$. We shall show by induction on j, $2 \le j \le p$, that there exists $\beta_j \in H^2(N,\mathbb{F}_p)$ such that

$$(\sigma-1)^{j-1}\beta_j = \gamma.$$

Then for β_p we shall have

$$(\sigma-1)^{p-1}\beta_p = \gamma \in (\sigma-1)^{p-1}H^2(N,\mathbb{F}_p),$$

which will prove our desired inclusion

$$H^2(N,\mathbb{F}_p)^{G/N} \cap (\sigma-1)H^2(N,\mathbb{F}_p) \subset (\sigma-1)^{p-1}H^2(N,\mathbb{F}_p).$$

If $j = 2$ we set $\beta_2 = \beta$. Assume now that $2 \leq j-1 < p$ and that $(\sigma-1)^{j-2}\beta_{j-1} = \gamma$ for some $\beta_{j-1} \in H^2(N, \mathbb{F}_p)$. Consider $\delta = \operatorname{cor}\beta_{j-1}$. Since

$$(\sigma-1)^{j-1}\beta_{j-1} = (\sigma-1)\gamma = 0$$

and $(\sigma-1)^{p-1} = \operatorname{res}\operatorname{cor}$, we obtain $\operatorname{res}\operatorname{cor}\beta_{j-1} = \operatorname{res}\delta = 0$. By Proposition 2, part (3), $\delta = (a)\cdot(f)$ for $(f) \in H^1(G, \mathbb{F}_p)$. By Lemma 1 there exists an element $x \in H^2(N, \mathbb{F}_p)^{G/N}$ such that $\operatorname{cor} x = (a)\cdot(f)$. Let $\beta'_{j-1} = \beta_{j-1} - x$.

From $(\sigma-1)x = 0$ and $j > 2$ we obtain

$$(\sigma-1)^{j-2}\beta'_{j-1} = (\sigma-1)^{j-2}\beta_{j-1} = \gamma.$$

Moreover $\operatorname{cor}\beta'_{j-1} = 0$. By the Corollary to Proposition 2, there exists $\beta_j \in H^2(N, \mathbb{F}_p)$ such that $(\sigma-1)\beta_j = \beta'_{j-1}$ and hence

$$(\sigma-1)^{j-1}\beta_j = (\sigma-1)^{j-2}\beta'_{j-1} = \gamma,$$

as desired. □

Lemma 3. *Let H be a cyclic group of order p generated by σ, and let T be an $\mathbb{F}_p[H]$-module. Suppose that $\alpha \in T$ and $(\sigma-1)^{p-1}\alpha \neq 0$. Then the $\mathbb{F}_p[H]$-submodule $\langle\alpha\rangle$ of T generated by α is a free $\mathbb{F}_p[H]$-module.*

Proof. Let $S = \mathbb{F}_p[H]$ and let I be any nonzero ideal of S. Let $w \neq 0$ be in I. Write

$$w = \sum_{i=k}^{p-1} c_i(\sigma-1)^i, \quad k \in \{0, 1, \ldots, p-1\},\ c_i \in \mathbb{F}_p,\ c_k \neq 0.$$

Then also $w(\sigma-1)^{p-1-k} = c_k(\sigma-1)^{p-1} \in I$, and hence $(\sigma-1)^{p-1} \in I$.

Now consider $\operatorname{ann}_S(\alpha) = \{s \in S \mid s\alpha = 0\}$. If $\operatorname{ann}_S(\alpha) \neq \{0\}$ then $(\sigma-1)^{p-1} \in \operatorname{ann}_S(\alpha)$, contradicting our hypothesis. Hence $\operatorname{ann}_S(\alpha) = \{0\}$ and we see that $\langle\alpha\rangle$ is a free $\mathbb{F}_p[H]$-submodule of T. □

Proof of Theorem 3. By Lemma 1, there exists a trivial $\mathbb{F}_p[G/N]$-submodule X of $H^2(N, \mathbb{F}_p)$ such that $\operatorname{cor} : X \to (a)\cdot H^1(G, \mathbb{F}_p)$ is an isomorphism. Hence $\dim_{\mathbb{F}_p} X = \dim_{\mathbb{F}_p}\ H^1(G, \mathbb{F}_p)/\operatorname{ann}(a)$. (Recall that $\operatorname{ann}(a) = \{(b) \in H^1(G, \mathbb{F}_p) \mid (a)\cdot(b) = 0\}$.)

Furthermore, there exists a maximal free $\mathbb{F}_p[G/N]$-submodule Y of $H^2(N, \mathbb{F}_p)$, as follows. (Y may be zero since we consider $\{0\}$ to be a free $\mathbb{F}_p[G/N]$-module.) First by [La, §III.1, Proposition 1.4], an $\mathbb{F}_p[G/N]$-module M is free precisely when $H^2(G/N, M) = \{0\}$. Observe that the trace map $1 + \sigma + \cdots + \sigma^{p-1} = (\sigma-1)^{p-1}$ in $\mathbb{F}_p[G/N]$. Recall that for any $\mathbb{F}_p[G/N]$-module M we have $H^2(G/N, M) = M^{G/N}/(\sigma-1)^{p-1}M$. (See [La, I.5].) Therefore M is a free $\mathbb{F}_p[G/N]$-module if and only if $M^{G/N} = (\sigma-1)^{p-1}M$. Let $\mathcal{S}$ denote the set of free $\mathbb{F}_p[G/N]$-submodules of $H^2(N, \mathbb{F}_p)$. Suppose $\mathcal{T}$ is a totally ordered subset of $\mathcal{S}$, and let $W = \cup_{S\in\mathcal{T}} S$. Then W is the inductive limit of $S \in \mathcal{T}$. Thus we have:

$$H^2(G/N, W) = H^2(G/N, \varinjlim_{S\in\mathcal{T}} S) = \varinjlim_{S\in\mathcal{T}} H^2(G/N, S) = \{0\}.$$

Hence W is a free $\mathbb{F}_p[G/N]$-module. By Zorn's Lemma, $\mathcal{S}$ contains a maximal element Y. We then have $Y^{G/N} = (\sigma-1)^{p-1}Y$. Since $\dim_{\mathbb{F}_p} \mathbb{F}_p[G/N]^{G/N} = \dim_{\mathbb{F}_p}\langle(\sigma-1)^{p-1}\rangle = 1$, we obtain

$$\operatorname{rank} Y = \dim_{\mathbb{F}_p} Y^{G/N} = \dim_{\mathbb{F}_p}(\sigma-1)^{p-1}Y.$$

Because free $\mathbb{F}_p[G/N]$-modules are injective (see [C, Theorem 11.2]) we may write $H^2(N, \mathbb{F}_p) = Y \oplus R$ for some $\mathbb{F}_p[G/N]$-submodule R of $H^2(N, \mathbb{F}_p)$. We will show that $R \cong X$ as $\mathbb{F}_p[G/N]$-modules.

We first show that R is a trivial $\mathbb{F}_p[G/N]$-module. If there exists $\alpha \in R$ with $(\sigma-1)^{p-1}\alpha \neq 0$, by Lemma 3 we see that $Y \oplus \langle\alpha\rangle$ is a larger free $\mathbb{F}_p[G/N]$-submodule, a contradiction. We obtain $(\sigma-1)^{p-1}R = \{0\}$ and $(\sigma-1)^{p-1}Y = (\sigma-1)^{p-1}H^2(N, \mathbb{F}_p)$.

Because $(\sigma-1)^{p-1}R = \{0\}$ there exists a minimal $0 \leq l \leq p-1$ such that $(\sigma-1)^l R = \{0\}$. Suppose $l > 1$. Then

$$\{0\} \neq (\sigma-1)^{l-1}R \subset H^2(N, \mathbb{F}_p)^{G/N} \cap (\sigma-1)H^2(N, \mathbb{F}_p).$$

By Lemma 2,

$$\{0\} \neq (\sigma-1)^{l-1}R \subset (\sigma-1)^{p-1}H^2(N, \mathbb{F}_p) = (\sigma-1)^{p-1}Y.$$

But then $\{0\} \neq (\sigma-1)^{l-1}R \subset R \cap Y$, a contradiction. Therefore $l \leq 1$ and $(\sigma-1)R = \{0\}$. Hence R is indeed a trivial $\mathbb{F}_p[G/N]$-module.

In fact, we claim that $R \cap (\sigma-1)H^2(N, \mathbb{F}_p) = \{0\}$. We have

$$\begin{aligned} R \cap (\sigma-1)H^2(N, \mathbb{F}_p) &\subset H^2(N, \mathbb{F}_p)^{G/N} \cap (\sigma-1)H^2(N, \mathbb{F}_p) \\ &= (\sigma-1)^{p-1}H^2(N, \mathbb{F}_p) = (\sigma-1)^{p-1}Y. \end{aligned}$$

From $R \cap Y = \{0\}$ we obtain $R \cap (\sigma-1)H^2(N, \mathbb{F}_p) = \{0\}$.

Now consider the image of cor on

$$H^2(N, \mathbb{F}_p)^{G/N} = R \oplus Y^{G/N} = R \oplus (\sigma-1)^{p-1}H^2(N, \mathbb{F}_p).$$

Observe that since the corestriction commutes with σ [NSW, Proposition 1.5.4], cor vanishes on the image of $\sigma - 1$. By Lemma 1, we find that $\operatorname{cor} R = (a) \cdot H^1(G, \mathbb{F}_p) = \operatorname{cor} X$. But by the Corollary to Proposition 2 and the fact that $R \cap (\sigma - 1)H^2(N, \mathbb{F}_p) = \{0\}$, we deduce that cor acts injectively on R. Since, by Lemma 1, cor also acts injectively on X, we have that $R \cong X$. Hence we obtain that $H^2(N, \mathbb{F}_p) \cong X \oplus Y$.

Now we determine the rank of Y. We have $(\sigma - 1)^{p-1} H^2(N, \mathbb{F}_p) = (\sigma - 1)^{p-1} Y$, and hence

$$\operatorname{rank} Y = \dim_{\mathbb{F}_p} (\sigma - 1)^{p-1} H^2(N, \mathbb{F}_p).$$

Using the hypothesis $\operatorname{cor} H^2(N, \mathbb{F}_p) = H^2(G, \mathbb{F}_p)$ together with $\operatorname{res} \operatorname{cor} = (\sigma - 1)^{p-1}$, we obtain that $(\sigma - 1)^{p-1} H^2(N, \mathbb{F}_p) = \operatorname{res} H^2(G, \mathbb{F}_p)$. By Proposition 2, part (3), the kernel of res is $(a) \cdot H^1(G, \mathbb{F}_p)$. We deduce then that $\operatorname{rank} Y = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)/(a) \cdot H^1(G, \mathbb{F}_p)$. □

Theorem 4. *Let F be a field containing a primitive p-th root of unity, and suppose that $G = \operatorname{Gal}(F(p)/F)$. Let N be a subgroup of G of index p, and suppose that the corestriction map* $\operatorname{cor} : H^2(N, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ *is surjective.*

Suppose that X and Y are $\mathbb{F}_p[G/N]$-submodules of $H^2(N, \mathbb{F}_p)$ such that X trivial and Y is free. Then $\operatorname{cor} X \subset (a) \cdot H^1(G, \mathbb{F}_p)$ *and the following are equivalent:*

(1) $\operatorname{cor} : X \to (a) \cdot H^1(G, \mathbb{F}_p)$ *is an isomorphism, and Y is a maximal free submodule*
(2) $H^2(N, \mathbb{F}_p) = X \oplus Y$.

Proof. Since X is a trivial $\mathbb{F}_p[G/N]$-module, $\operatorname{res} \operatorname{cor} X = (\sigma - 1)^{p-1} X = \{0\}$. By Proposition 2, part (3), $\operatorname{cor} X \subset (a) \cdot H^1(G, \mathbb{F}_p)$.

(1) $\Longrightarrow$ (2). Suppose $w \in X \cap Y$. Since X is a trivial $\mathbb{F}_p[G/N]$-module, $w \in Y^{G/N}$. Then because Y is a free $\mathbb{F}_p[G/N]$-module, $Y^{G/N} = (\sigma - 1)^{p-1} Y$. In particular, $w \in (\sigma - 1)Y$. Since cor vanishes on the image of $\sigma - 1$, $\operatorname{cor} w = 0$, and because cor is injective on X, $w = 0$. Hence the submodule of $H^2(G, \mathbb{F}_p)$ generated by X and Y is $X \oplus Y$.

Let R be a trivial $\mathbb{F}_p[G/N]$-submodule of $H^2(N, \mathbb{F}_p)$ such that $\operatorname{cor} R = \operatorname{cor} X$ and $H^2(N, \mathbb{F}_p) = R \oplus Y$, as in the proof of Theorem 3. Since $(\sigma - 1)R = \{0\}$ we deduce that $(\sigma - 1)^{p-1} Y = (\sigma - 1)^{p-1} H^2(N, \mathbb{F}_p)$.

To prove that $X \oplus Y = H^2(N, \mathbb{F}_p)$ it suffices to prove that $R \subset X \oplus Y$. Let $r \in R$. Then there exists $x \in X$ such that $\operatorname{cor} r = \operatorname{cor} x$.

Thus $u = r - x \in H^2(N, \mathbb{F}_p)^{G/N}$ and $\operatorname{cor} u = 0$. By the Corollary to Proposition 2 we obtain that $u \in (\sigma - 1)H^2(N, \mathbb{F}_p)$. Thus

$$u \in H^2(N, \mathbb{F}_p)^{G/N} \cap (\sigma - 1)H^2(N, \mathbb{F}_p),$$

and so by Lemma 2,

$$u \in (\sigma - 1)^{p-1}H^2(N, \mathbb{F}_p) = (\sigma - 1)^{p-1}Y.$$

Hence $r \in X \oplus Y$ as required and we have $X \oplus Y = H^2(N, \mathbb{F}_p)$.

(2) $\implies$ (1). By Lemma 1, $\operatorname{cor}(H^2(N, \mathbb{F}_p)^{G/N}) = (a) \cdot H^1(G, \mathbb{F}_p)$. Since Y is free, $Y^{G/N} = (\sigma - 1)^{p-1}Y$, and since cor vanishes on the image of $\sigma - 1$, $\operatorname{cor} Y^{G/N} = \{0\}$. From $H^2(N, \mathbb{F}_p)^{G/N} = X \oplus Y^{G/N}$ we deduce that $\operatorname{cor} : X \to (a) \cdot H^1(G, \mathbb{F}_p)$ is surjective. Now if $x \in X$ with $\operatorname{cor} x = 0$ then by the Corollary to Proposition 2, $x \in (\sigma - 1)H^2(N, \mathbb{F}_p)$. Because X is trivial and $X \oplus Y = H^2(N, \mathbb{F}_p)$, we see that

$$\begin{aligned} x &\in (\sigma - 1)H^2(N, \mathbb{F}_p) \cap H^2(N, \mathbb{F}_p)^{G/N} \\ &= (\sigma - 1)^{p-1}H^2(N, \mathbb{F}_p) = (\sigma - 1)^{p-1}Y \end{aligned}$$

by Lemma 2. Then $x \in X \cap Y$, and so $x = 0$. Hence cor is injective on X and therefore $\operatorname{cor} : X \to (a) \cdot H^1(G, \mathbb{F}_p)$ is an isomorphism.

Finally we show that Y is a maximal free $\mathbb{F}_p[G/N]$-submodule. Suppose $Y \subset T$ where T is a free $\mathbb{F}_p[G/N]$-submodule of $H^2(N, \mathbb{F}_p)$. Then because Y is injective we can write $T = Y \oplus S$ for some $\mathbb{F}_p[G/N]$-module S. Then S is a projective $\mathbb{F}_p[G/N]$-module, and since each projective $\mathbb{F}_p[G/N]$-module is free (see [C, Proof of Theorem 11.2, pp. 70–71]) we see that S is in fact a free $\mathbb{F}_p[G/N]$-submodule of T. Then we have

$$\begin{aligned} \operatorname{res}\operatorname{cor} T &= \operatorname{res}\operatorname{cor} Y \oplus \operatorname{res}\operatorname{cor} S \\ &= (\sigma - 1)^{p-1}Y \oplus (\sigma - 1)^{p-1}S. \end{aligned}$$

But since $H^2(N, \mathbb{F}_p) = X \oplus Y$ and X is a trivial $\mathbb{F}_p[G/N]$-submodule of $H^2(N, \mathbb{F}_p)$ we see that

$$\begin{aligned} \operatorname{res}\operatorname{cor} H^2(N, \mathbb{F}_p) &= (\sigma - 1)^{p-1}H^2(N, \mathbb{F}_p) \\ &= (\sigma - 1)^{p-1}Y. \end{aligned}$$

Hence $(\sigma - 1)^{p-1}S = \{0\}$. Since S is free, $S = \{0\}$. Thus Y is indeed a maximal free $\mathbb{F}_p[G/N]$-submodule of $H^2(N, \mathbb{F}_p)$. $\square$

5. Proof of Theorem 1

Let N be a subgroup of G of index p. Since G has cohomological dimension 2, the corestriction map $\mathrm{cor} : H^2(N, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is surjective [NSW, Proposition 3.3.8]. By Theorem 3 we have a decomposition $H^2(N, \mathbb{F}_p) = X \oplus Y$, where X is a trivial $\mathbb{F}_p[G/N]$-module and Y is a free $\mathbb{F}_p[G/N]$-module. Hence $H^2(N, \mathbb{F}_p)$ is trivial if and only if $H^2(N, \mathbb{F}_p)$ contains no nonzero free submodule. We have established the first equivalence of the theorem.

For the next assertion, observe that if G is a Demuškin group of cohomological dimension 2 and N is a subgroup of G of index p, by [DuLa, Theorem 1], the $\mathbb{F}_p[G/N]$-module $H^2(N, \mathbb{F}_p)$ is a trivial $\mathbb{F}_p[G/N]$-module.

Conversely, by the definition of a Demuškin group, it suffices to show that $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$ and γ_F is nondegenerate. Consider the decomposition $H^2(N, \mathbb{F}_p)$ obtained above, for N an arbitrary subgroup of index p. Let $a \in F^\times$ be chosen so that the fixed field of N is $F(\sqrt[p]{a})$. Since we are assuming that $H^2(N, \mathbb{F}_p)$ contains no nonzero free summand, from Theorem 3 we obtain $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)/(a) \cdot H^1(G, \mathbb{F}_p) = 0$, or $(a) \cdot H^1(G, \mathbb{F}_p) = H^2(G, \mathbb{F}_p)$. Hence γ_F is strongly regular. Moreover, $H^2(N, \mathbb{F}_p)$ has $\mathbb{F}_p$-dimension

$$\begin{aligned}\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)/\mathrm{ann}(a) &= \dim_{\mathbb{F}_p} \big((a) \cdot H^1(G, \mathbb{F}_p)\big) \\ &= \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p).\end{aligned}$$

Suppose that the pairing γ_F is degenerate. Then for some nonzero $(a) \in H^1(G, \mathbb{F}_p)$ we have $(a) \cdot H^1(G, \mathbb{F}_p) = \{0\}$. Then $H^2(G, \mathbb{F}_p) = \{0\}$, contradicting the cohomological dimension of G. Hence γ_F is nondegenerate. Now if $p = 2$ we have $H^2(G, \mathbb{F}_2) \cong \mathbb{F}_2$ by Proposition 1. If $p > 2$ and we assume the Elementary Type Conjecture, then by Theorem 2, γ_F is of p-local type and hence $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$.

Thus G is a Demuškin group as required. □

Remark 1. In the proof of Theorem 1 we cited [DuLa, Theorem 1] to establish that if G is Demuškin with $\mathrm{cd}(G) = 2$, then $H^2(N, \mathbb{F}_p)$ is a trivial $\mathbb{F}_p[G/N]$-module. This result also follows from the fact that open subgroups of Demuškin groups $G \neq \mathbb{Z}/2\mathbb{Z}$ are also Demuškin [S, Corollary I.4.5]. We observe that we can also deduce this result in our setting when $G = \mathrm{Gal}(F(p)/F)$ from Theorem 3, as follows. By Theorem 3, $H^2(N, \mathbb{F}_p)$ is the direct sum of a trivial $\mathbb{F}_p[G/N]$-module X and a free $\mathbb{F}_p[G/N]$-module Y. Since G is Demuškin, γ_F is strongly regular. From Theorem 3(2), we have $Y = \{0\}$. Hence $H^2(N, \mathbb{F}_p)$ is a trivial $\mathbb{F}_p[G/N]$-module as required. More precisely, from Theorem 3(1) and the fact that γ_F is strongly regular we obtain $H^2(N, \mathbb{F}_p) \cong X \cong \mathbb{F}_p$.

Remark 2. By Theorem 2, the Elementary Type Conjecture for Odd p holds for a field F with a strongly regular non-totally degenerate p-quaternionic pairing γ_F if and only if $G = \mathrm{Gal}(F(p)/F)$ is Demuškin. Thus Theorem 1 may be viewed as a translation of the Elementary Type Conjecture to the language of Galois $\mathbb{F}_p[G/N]$-modules $H^2(N, \mathbb{F}_p)$ in the case of strongly regular non-totally degenerate p-quaternionic pairings. There is some additional interest in this formulation because p-quaternionic pairings which are strongly regular but not weakly p-local have been abstractly constructed (see [Ku2, Theorem 9]), and it is not known whether these pairings are realizable as γ_F for suitable fields F.

6. Structure of $H^1(N, \mathbb{F}_p)$

In this section we keep our assumption that a primitive p-th root of unity lies in F. For any finitely generated pro-p-group T we set $d(T) = \dim_{\mathbb{F}_p} H^1(T, \mathbb{F}_p)$.

If G is a Demuškin pro-p-group then it is well-known that

$$d(N) = p(d(G) - 2) + 2$$

for any subgroup N of index p of G. Moreover this formula characterizes Demuškin groups among finitely generated pro-p-groups G with $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$. (See [DuLa] or [NSW, Theorem 3.9.15].) In this section we show that this formula has an attractive explanation when $G = \mathrm{Gal}(F(p)/F)$. In the following theorem K is the fixed field in $F(p)$ of the index p subgroup N of G.

Theorem 5. *Let F be a field containing a primitive p-th root of unity ξ_p, and suppose that $G = \mathrm{Gal}(F(p)/F)$ is a Demuškin group of rank $d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = n$.*

If $p > 2$, then for each subgroup N of G of index p we have a decomposition into $\mathbb{F}_p[G/N]$-modules

$$H^1(N, \mathbb{F}_p) = X \oplus Y$$

where X is an $\mathbb{F}_p[G/N]$-module of dimension 2 and Y is a free $\mathbb{F}_p[G/N]$-module of rank $n - 2$. The module X is trivial if $\xi_p \in N_{K/F}(K^\times)$ and is cyclic of dimension 2 otherwise.

If $p = 2$ then for each subgroup N of G of index p we have one of two decompositions into $\mathbb{F}_2[G/N]$-modules

$$H^1(N, \mathbb{F}_2) = X \oplus Y \quad \textit{or} \quad H^1(N, \mathbb{F}_2) = Y.$$

The first case occurs when $-1 \in N_{K/F}(K^\times)$, and then X is trivial of dimension 2 and Y is free of rank $n-2$. The second occurs when $-1 \notin N_{K/F}(K^\times)$, and then Y is free of rank $n-1$.

Proof. Observe that for N an index p subgroup of the Demuškin group G and K its fixed field in $F(p)$, we have $\dim_{\mathbb{F}_p} F^\times/N_{K/F}(K^\times) = 1$. Using equivariant Kummer theory, as explained in [W2], to identify the first cohomology groups with their corresponding pth-power classes as $\mathbb{F}_p[G/N]$-modules, the result then follows from the determination of the $\mathbb{F}_p[G/N]$-module structure of $K^\times/K^{\times p}$ in [MiSw, Theorem 3]. □

Acknowledgements

We thank Professors I. Efrat, M. Kula, J.-P. Serre, and the referee for their careful reading of preliminary versions of this paper and for their valuable comments and suggestions. We are also grateful to M. Fried for his encouragement and infectious enthusiasm regarding this research.

References

[C] J. Carlson. *Modules and group algebras.* Lectures in Mathematics ETH Zürich. Basel: Birkhäuser Verlag, 1996.

[DuLa] D. Dummit and J. Labute. On a new characterization of Demuškin groups. *Invent. Math.* **73** (1983), no. 3, 413–418.

[Ef1] I. Efrat. Pro-p Galois groups of algebraic extensions of $\mathbb{Q}$. *J. Number Theory* **64** (1997), no. 1, 84–99.

[Ef2] I. Efrat. Finitely generated pro-p absolute Galois groups over global fields. *J. Number Theory* **77** (1999), no. 1, 83–96.

[Ef3] I. Efrat. Demuškin fields with valuations. *Math. Z.* **243** (2003), no. 2, 333–353.

[En] A. Engler. A recursive description of pro-p Galois groups. *J. Algebra* **274** (2004), no. 2, 511–522.

[FY] R. Fitzgerald and J. Yucas. Combinatorial techniques and abstract Witt rings I. *J. Algebra* **114** (1988), 40–52.

[HJ] Y. S. Hwang and B. Jacob. Brauer group analogues of results relating the Witt ring to valuations and Galois theory. *Canad. J. Math.* **47** (1995), no. 3, 527–543.

[JW] B. Jacob and R. Ware. A recursive description of the maximal pro-2 Galois group via Witt rings. *Math. Z.* **200** (1989), no. 3, 379–396.

[Ko] J. Koenigsmann. Encoding valuations in absolute Galois groups. *Proceedings of the international conference and workshop on Valuation Theory (Saskatoon, 1999)*, edited by F.-V. Kuhlmann, S. Kuhlmann, and M. Marshall, 107–132. Fields Institute Communications 33. Providence, RI: American Mathematical Society, 2003.

[Ku1] M. Kula. *Finitely generated Witt rings.* Scientific Publications of the University of Silesia 1207. Katowice: Uniwersytet Slaski, 1991.

[Ku2] M. Kula. On p-quaternionic pairings of non-elementary type. *Manuscripta Math.* **101** (2000), no. 1, 39–47.

[L] T.-Y. Lam. *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics 67. Providence, RI: American Mathematical Society, 2005.

[La] S. Lang. *Topics in cohomology of groups.* Lecture Notes in Mathematics 1625. Berlin: Springer-Verlag, 1996.

[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? *New York J. Math.* **11** (2005), 291–302.

[Ma1] M. Marshall. *Abstract Witt rings.* Queen's Papers in Pure and Applied Mathematics 57. Kingston, Canada: Queen's University, 1980.

[Ma2] M. Marshall. The elementary type conjecture in quadratic form theory. *Contemp. Math.* **344** (2004), 275–293.

[Me] A. Merkurjev. K_2 and the Brauer group. *Contemp. Math.* **55** (1986), 529–547.

[MeSu] A. S. Merkurjev and A. A. Suslin. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat.* **46** (1982), no. 5, 1011–1046, 1135–1136. English translation, *Math. USSR-Izv.* **21** (1983), no. 2, 307–340.

[MiSw] J. Mináč and J. Swallow. Galois module structure of pth-power classes of extensions of degree p. *Israel J. Math.* **138** (2003), 29–42.

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields.* Berlin: Springer-Verlag, 2000.

[S] J.-P. Serre. *Galois cohomology.* Berlin: Springer-Verlag, 2002.

[W1] W. Waterhouse. Profinite groups are Galois groups. *Proc. Amer. Math. Soc.* **42** (1973), 639–640.

[W2] W. Waterhouse. The normal closures of certain Kummer extensions. *Canad. Math. Bull.* **37** (1994), no. 1, 133–139.

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