# QUOTIENTS OF ABSOLUTE GALOIS GROUPS WHICH DETERMINE THE ENTIRE GALOIS COHOMOLOGY

SUNIL K. CHEBOLU, IDO EFRAT, AND JÁN MINÁČ

ABSTRACT. For prime power $q = p^d$ and a field $F$ containing a root of unity of order $q$ we show that the Galois cohomology ring $H^*(G_F, \mathbb{Z}/q)$ is determined by a quotient $G_F^{[3]}$ of the absolute Galois group $G_F$ related to its descending $q$-central sequence. Conversely, we show that $G_F^{[3]}$ is determined by the lower cohomology of $G_F$. This is used to give new examples of pro-$p$ groups which do not occur as absolute Galois groups of fields.

## 1. INTRODUCTION

A main open problem in modern Galois theory is the characterization of the profinite groups which are realizable as absolute Galois groups of fields $F$. The torsion in such groups is described by the Artin–Schreier theory from the late 1920's, namely, it consists solely of involutions. More refined information on the structure of absolute Galois groups is given by Galois cohomology, systematically developed starting the 1950's by Tate, Serre, and others. Yet, explicit examples of torsion-free profinite groups which are not absolute Galois groups are rare. In 1970, Milnor [Mil70] introduced his $K$-ring functor $K_*^M(F)$, and pointed out close connections between this graded ring and the mod-2 Galois cohomology of the field. This connection, in a more general form, became known as the Bloch–Kato conjecture: it says that for all $r \geq 0$ and all $m$ prime to char $F$, there is a canonical isomorphism $K_r^M(F)/m \to H^r(G_F, \mu_m^{\otimes r})$ ([GS06]; see notation below). The conjecture was proved for $r = 2$ by Merkurjev and Suslin [MS82], for $r$ arbitrary and $m = 2$ by Voevodsky [Voe03a], and in general by Rost, Voevodsky, with a patch by Weibel ([Voe03b], [Wei09], [Wei08], [HW09]).

In this paper we obtain new constrains on the group structure of absolute Galois groups of fields, using this isomorphism. We use these constrains to produce new examples of torsion-free profinite groups which are not absolute Galois groups. We also demonstrate that the maximal pro-$p$ quotient of the absolute Galois group can be characterized in purely cohomological terms. The main object of our paper is a remarkable small quotient of the absolute Galois group, which, because of the above isomorphism, already carries a substantial information about the arithmetic of $F$.

More specifically, fix a prime number $p$ and a $p$-power $q = p^d$, with $d \geq 1$. All fields which appear in this paper will be tacitly assumed to contain a primitive $q$th root of

2000 *Mathematics Subject Classification.* Primary 12G05; Secondary 12F10, 12E30.

*Key words and phrases.* absolute Galois group, Galois cohomology, descending central sequence, $W$-group.

Ján Mináč was supported in part by National Sciences and Engineering Council of Canada grant R0370A01.

unity. Let $F$ be such a field and let $G_F = \mathrm{Gal}(F_{\mathrm{sep}}/F)$ be its absolute Galois group, where $F_{\mathrm{sep}}$ is the separable closure of $F$. Let $H^*(G_F) = H^*(G_F, \mathbb{Z}/q)$ be the Galois cohomology ring with the trivial action of $G_F$ on $\mathbb{Z}/q$. Our new constraints relate the descending $q$-central sequence $G_F^{(i)}$, $i = 1, 2, 3, \ldots$, of $G_F$ (see §4) with $H^*(G_F)$. Setting $G_F^{[i]} = G_F/G_F^{(i)}$, we show that the quotient $G_F^{[3]}$ determines $H^*(G_F)$, and vice versa. Specifically, we prove:

**Theorem A.** *The inflation map gives an isomorphism*

$$H^*(G_F^{[3]})_{\mathrm{dec}} \xrightarrow{\sim} H^*(G_F),$$

*where $H^*(G_F^{[3]})_{\mathrm{dec}}$ is the decomposable part of $H^*(G_F^{[3]})$ (i.e., its subring generated by degree 1 elements).*

We further have the following converse results.

**Theorem B.** *$G_F^{[3]}$ is uniquely determined by $H^r(G_F)$ for $r = 1, 2$, the cup product $\cup\colon H^1(G_F) \times H^1(G_F) \to H^2(G_F)$ and the Bockstein homomorphism $\beta\colon H^1(G_F) \to H^2(G_F)$ (see §2 for the definition of $\beta$).*

**Theorem C.** *Let $F_1$, $F_2$ be fields and let $\pi\colon G_{F_1} \to G_{F_2}$ be a (continuous) homomorphism. The following conditions are equivalent:*

(i) *the induced map $\pi^*\colon H^*(G_{F_2}) \to H^*(G_{F_1})$ is an isomorphism;*

(ii) *the induced map $\pi^{[3]}\colon G_{F_1}^{[3]} \to G_{F_2}^{[3]}$ is an isomorphism.*

Theorems A–C show that $G_F^{[3]}$ is a Galois-theoretic analog of the cohomology ring $H^*(G_F)$. Its structure is considerably simpler and more accessible than the full absolute Galois group $G_F$ (see e.g., [EM07]). Yet, as shown in our theorems, these small and accessible quotients encode and control the entire cohomology ring. Results similar to Theorems A–C are valid in a relative pro-$p$ setting, where one replaces $G_F$ by its maximal pro-$p$ quotient $G_F(p) = \mathrm{Gal}(F(p)/F)$ (here $F(p)$ is the compositum of all finite Galois extensions of $F$ of $p$-power order; see Remark 8.2).

In the case $q = 2$ the group $G_F^{[3]}$ has been extensively studied under the name "$W$-group", in particular in connection with quadratic forms ([Spi87], [MSp90], [MSp96], [AKM99], [MMS04]). In this special case, Theorem A was proved in [AKM99, Th. 3.14]. It was further shown that then $G_F^{[3]}$ has great arithmetical significance: it encodes large parts of the arithmetical structure of $F$, such as its orderings, its Witt ring, and certain non-trivial valuations. Theorem A explains this surprising phenomena, as these arithmetical objects are known to be encoded in $H^*(G_F)$ (with the additional knowledge of the Kummer element of $-1$).

First links between these quotients and the Bloch–Kato conjecture, and its special case the Merkurjev–Suslin theorem, were already noticed in a joint work of Mináč and Spira in [Spi87] and in Bogomolov's paper [Bog92]. The latter paper was the first in a remarkable line of works by Bogomolov and Tschinkel ([Bog92], [BT08], [BT09]), as well as by Pop (unpublished), focusing on the closely related quotient $G_F/[G_F, [G_F, G_F]]$ (the analog of $G_F^{[3]}$ for $q = 0$), where $F$ is a function field over an algebraically closed field. There the viewpoint is that of "birational anabelian geometry": namely, it is shown that for certain important classes of such function fields, $F$ itself is determined by this quotient. Our work, on the other hand, is aimed at clarifying the structure of the smaller Galois group $G_F^{[3]}$ and its connections with the Galois cohomology and arithmetic of almost arbitrary fields, focusing on the structure of absolute Galois groups.

Our approach is purely group-theoretic, and the main results above are in fact proved for arbitrary profinite groups which satisfy certain conditions on their cohomology (Theorem 6.5, Proposition 7.3 and Theorem 6.3). A key point is a rather general group-theoretic approach, partly inspired by [GM97], to the Milnor $K$-ring construction by means of quadratic hulls of graded algebras (§3). The Rost–Voevodsky theorem on the bijectivity of the Galois symbol shows that these cohomological conditions are satisfied by absolute Galois groups as above. Using this we deduce in §9 Theorems A–C in their field-theoretic version.

We thank L. Avramov, T. Chinburg, J.-L. Colliot-Thélène, W.-D. Geyer, P. Goerss, M. Jarden, P. May, and T. Szamuely for their comments related to talks on this work given at the 2009 Field Arithmetic meeting in Oberwolfach, the University of Chicago, Northwestern University, and the University of Nebraska, Lincoln.

## 2. Cohomological preliminaries

We work in the category of profinite groups. Thus subgroups are always tacitly assumed to be closed and homomorphism are assumed to be continuous. For basic facts on Galois cohomology we refer e.g., to [NSW08], [Ser02], or [Koc02]. We abbreviate $H^r(G) = H^r(G, \mathbb{Z}/q)$ with the trivial $G$-action on $\mathbb{Z}/q$. Let $H^*(G) = \bigoplus_{r=0}^{\infty} H^r(G)$ be the graded cohomology ring with the cup product. We write res, inf, and trg for the restriction, inflation, and transgression maps. Given a homomorphism $\pi\colon G_1 \to G_2$ of profinite groups, we write $\pi^*\colon H^*(G_2) \to H^*(G_1)$ and $\pi^*_r\colon H^r(G_2) \to H^r(G_1)$ for the induced homomorphisms. The **Bockstein homomorphism** $\beta\colon H^1(G) \to H^2(G)$ of $G$ is the connecting homomorphism arising from the short exact sequence of trivial $G$-modules

$$0 \to \mathbb{Z}/q \to \mathbb{Z}/q^2 \to \mathbb{Z}/q \to 0.$$

When $q = 2$ one has $\beta(\psi) = \psi \cup \psi$ [EM07, Lemma 2.4].

Given a normal subgroup $N$ of $G$, there is a natural action of $G$ on $H^r(N)$. For $r = 1$ it is given by $\varphi \mapsto \varphi^g$, where $\varphi^g(n) = \varphi(g^{-1}ng)$ for $\varphi \in H^1(N)$, $g \in G$ and $n \in N$. Let $H^r(N)^G$ be the group of all $G$-invariant elements of $H^r(N)$. Recall that there is a 5-term exact sequence

$$0 \to H^1(G/N) \xrightarrow{\mathrm{inf}_G} H^1(G) \xrightarrow{\mathrm{res}_N} H^1(N)^G \xrightarrow{\mathrm{trg}_{G/N}} H^2(G/N) \xrightarrow{\mathrm{inf}_G} H^2(G),$$

which is functorial in $(G, N)$ in the natural sense.

## 3. Graded rings

Let $R$ be a commutative ring and $\mathcal{A} = \bigoplus_{r=0}^{\infty} A_r$ a graded associative $R$-algebra with $A_0 = R$. Assume that $\mathcal{A}$ is either commutative or graded-commutative (i.e., $ab = (-1)^{rs}ba$ for $a \in A_r$, $b \in A_s$). For $r \geq 0$ let $A_{\mathrm{dec},r}$ be the $R$-submodule of $A_r$ generated by all products of $r$ elements of $A_1$ (by convention $A_{\mathrm{dec},0} = R$). The graded $R$-subalgebra $\mathcal{A}_{\mathrm{dec}} = \bigoplus_{r=0}^{\infty} A_{\mathrm{dec},r}$ is the **decomposable part** of $\mathcal{A}$. We say that $A_r$ (resp., $\mathcal{A}$) is **decomposable** if $A_r = A_{\mathrm{dec},r}$ (resp., $\mathcal{A} = \mathcal{A}_{\mathrm{dec}}$).

Motivated by the Milnor $K$-theory of a field [Mil70], we define the quadratic hull $\hat{\mathcal{A}}$ of the algebra $\mathcal{A}$ as follows. For $r \geq 0$ let $T_r$ be the $R$-submodule of $A_1^{\otimes r}$ generated by all tensors $a_1 \otimes \cdots \otimes a_r$ such that $a_i a_j = 0 \in A_2$ for some distinct $1 \leq i, j \leq r$ (by convention, $A_1^{\otimes 0} = R$, $T_0 = 0$). We define $\hat{\mathcal{A}}$ to be the graded $R$-algebra $\hat{\mathcal{A}} = \bigoplus_{r=0}^{\infty} A_1^{\otimes r}/T_r$ with multiplicative structure induced by the tensor product. Because of the commutativity/graded-commutativity, there is a canonical graded $R$-algebra epimorphism $\omega_{\mathcal{A}} \colon \hat{\mathcal{A}} \to \mathcal{A}_{\mathrm{dec}}$, which is the identity map in degree 1. We call $\mathcal{A}$ **quadratic** if $\omega_{\mathcal{A}}$ is an isomorphism. Note that

$$\hat{\mathcal{A}} = (\hat{\mathcal{A}})_{\mathrm{dec}} = (\widehat{\mathcal{A}_{\mathrm{dec}}}).$$

These constructions are functorial in the sense that every graded $R$-algebra morphism $\varphi = (\varphi_r)_{r=0}^{\infty} \colon \mathcal{A} \to \mathcal{B}$ induces in a natural way graded $R$-algebra morphisms

$$\varphi_{\mathrm{dec}} = (\varphi_{\mathrm{dec},r})_{r=0}^{\infty} \colon \mathcal{A}_{\mathrm{dec}} \to \mathcal{B}_{\mathrm{dec}}, \qquad \hat{\varphi} = (\hat{\varphi}_r)_{r=0}^{\infty} \colon \hat{\mathcal{A}} \to \hat{\mathcal{B}}$$

with a commutative square

$$\begin{array}{ccc} \hat{\mathcal{A}} & \xrightarrow{\hat{\varphi}} & \hat{\mathcal{B}} \\ \downarrow{\scriptstyle \omega_{\mathcal{A}}} & & \downarrow{\scriptstyle \omega_{\mathcal{B}}} \\ \mathcal{A}_{\mathrm{dec}} & \xrightarrow{\varphi_{\mathrm{dec}}} & \mathcal{B}_{\mathrm{dec}}. \end{array} \tag{3.1}$$

The proof of the next fact is straightforward.

**Lemma 3.1.** *$\hat{\varphi}$ is an isomorphism if and only if $\varphi_1$ is an isomorphism and $\varphi_{\mathrm{dec},2}$ is a monomorphism.*

**Remark 3.2.** When $G$ is a profinite group, $R = \mathbb{Z}/2$, and $\mathcal{A} = H^*(G, \mathbb{Z}/2)$ the ring $\hat{\mathcal{A}}$ coincides with the ring $\mathrm{Mil}(G)$ introduced and studied in [GM97]. In the case where $G = G_F$ for a field $F$ as before, this ring is naturally isomorphic to $K_*^M(F)/2$. Thus in this way one can construct $K_*^M(F)/p$ for any $p$ in a purely group-theoretic way.

## 4. The descending central sequence

Let $G$ be a profinite group and let $q$ be either a $p$-power or 0. The **descending $q$-central sequence** of $G$ is defined inductively by

$$G^{(1,q)} = G, \quad G^{(i+1,q)} = (G^{(i,q)})^q [G^{(i,q)}, G], \quad i = 1, 2, \ldots .$$

Thus $G^{(i+1,q)}$ is the closed subgroup of $G$ topologically generated by all powers $h^q$ and all commutators $[h, g] = h^{-1}g^{-1}hg$, where $h \in G^{(i,q)}$ and $g \in G$. Note that $G^{(i,q)}$ is normal in $G$. For $i \geq 1$ let $G^{[i,q]} = G/G^{(i,q)}$. When $q = 0$ the sequence $G^{(i,0)}$ is called the **descending central sequence** of $G$. Usually $q$ will be fixed, and we will abbreviate

$$G^{(i)} = G^{(i,q)}, \ G^{[i]} = G^{[i,q]}.$$

Any profinite homomorphism (resp., epimorphism) $\pi \colon G \to H$ restricts to a homomorphism (resp., an epimorphism) $\pi^{(i)} \colon G^{(i)} \to H^{(i)}$. Hence $\pi$ induces a homomorphism (resp., an epimorphism) $\pi^{[i]} \colon G^{[i]} \to H^{[i]}$.

**Lemma 4.1.** *For $i, j \geq 1$ one has canonical isomorphisms*

(a) $(G^{[j]})^{(i)} \cong G^{(i)}/G^{(\max\{i,j\})}$;
(b) $(G^{[j]})^{[i]} \cong G^{[\min\{i,j\}]}$.

*Proof.* (a) Consider the natural epimorphism $\pi\colon G\to G^{[j]}$. Then $\pi^{(i)}\colon G^{(i)}\to (G^{[j]})^{(i)}$ is an epimorphism with kernel $G^{(i)}\cap \mathrm{Ker}(\pi)=G^{(i)}\cap G^{(j)}=G^{(\max\{i,j\})}$.

(b) By (a), there is a canonical isomorphism

$$(G^{[j]})^{[i]}\cong G^{[j]}/(G^{[j]})^{(i)}\cong (G/G^{(j)})/(G^{(i)}/G^{(\max\{i,j\})})\cong G^{[\min\{i,j\}]}. \qquad \square$$

**Lemma 4.2.** *Let $\pi\colon G_1\to G_2$ be a homomorphism of profinite groups. If $\pi^{[j]}$ is an epimorphism (resp., isomorphism), then $\pi^{[i]}$ is an epimorphism (resp., isomorphism) for all $i\leq j$.*

*Proof.* The assumption implies that $(\pi^{[j]})^{[i]}\colon (G_1^{[j]})^{[i]}\to (G_2^{[j]})^{[i]}$ is an epimorphism (resp., isomorphism). Now use Lemma 4.1(b). $\square$

**Lemma 4.3.** *Let $i\geq 1$ and let $N$ be a normal subgroup of $G$ with $N\leq G^{(i)}$ and $\pi\colon G\to G/N$ the natural map. Then $\pi^{[i]}$ is an isomorphism.*

*Proof.* Apply Lemma 4.1(b) with respect to the composed epimorphism $G\to G/N\to G^{[i]}$ to see that $\pi^{[i]}$ is injective. $\square$

**Lemma 4.4.** *Let $\pi\colon G_1\to G_2$ be an epimorphism of profinite groups. Then* $\mathrm{Ker}(\pi^{[i]})=\mathrm{Ker}(\pi)G_1^{(i)}/G_1^{(i)}$ *for all $i\geq 1$.*

*Proof.* The map $G_1\to G_2^{[i]}=\pi(G_1)/\pi(G_1)^{(i)}$ induced by $\pi$ has kernel $\mathrm{Ker}(\pi)G_1^{(i)}$, whence the assertion. $\square$

We will also need the following result of Labute [Lab66, Prop. 1 and 2] (see also [NSW08, Prop. 3.9.13]).

**Proposition 4.5.** *Let $S$ be a free pro-$p$ group on generators $\sigma_1,\dots,\sigma_n$. Consider the Lie $\mathbb{Z}_p$-algebra $\mathfrak{gr}(S)=\bigoplus_{i=1}^\infty S^{(i,0)}/S^{(i+1,0)}$, with Lie brackets induced by the commutator map. Then $\mathfrak{gr}(S)$ is a free Lie $\mathbb{Z}_p$-algebra on the images of $\sigma_1,\dots,\sigma_n$ in $\mathfrak{gr}_1(S)$. In particular, $S^{(2,0)}/S^{(3,0)}$ has a system of representatives consisting of all products $\prod_{1\leq k<l\leq n}[\sigma_k,\sigma_l]^{a_{kl}}$, where $a_{kl}\in\mathbb{Z}_p$.*

## 5. Duality

From now assume that $q=p^d$ with $p$ prime. One has

**Proposition 5.1** ([EM07, Cor. 2.2])**.** *For a normal subgroup $R$ of a profinite group $G$, there is a perfect duality*

$$R/R^q[R,G]\ \times\ H^1(R)^G\ \to\ \mathbb{Z}/q, \qquad (\bar r,\varphi)\mapsto\varphi(r).$$

We observe that this duality is functorial in the following sense:

**Proposition 5.2.** *For a homomorphism $\pi\colon G_1\to G_2$ of profinite groups and for normal subgroups $R_i$ of $G_i$, $i=1,2$, such that $\pi(R_1)\leq R_2$, the following induced diagram commutes in the natural sense:*

$$\begin{array}{ccccc}
R_1/R_1^q[R_1,G_1] & \times & H^1(R_1)^{G_1} & \longrightarrow & \mathbb{Z}/q\\
\Big\downarrow \overline{\pi|_{R_1}} & & \Big\uparrow (\pi|_{R_1})^*_1 & & \Big\| \\
R_2/R_2^q[R_2,G_2] & \times & H^1(R_2)^{G_2} & \longrightarrow & \mathbb{Z}/q.
\end{array}$$

We list some consequences of this duality.

**Lemma 5.3.** *Let $\pi\colon G_1 \to G_2$ be a homomorphism of profinite groups. Then $\pi^{[2]}$ is an isomorphism if and only if $\pi_1^*\colon H^1(G_2) \to H^1(G_1)$ is an isomorphism. In this case, $\pi^*_{\rm dec}\colon H^*(G_2)_{\rm dec} \to H^*(G_1)_{\rm dec}$ is surjective.*

*Proof.* For the equivalence use Proposition 5.2 with $G_i = R_i$, $i = 1, 2$. The second assertion follows from the first one. □

**Lemma 5.4.** res: $H^1(G^{(i)})^G \to H^1(G^{(i+1)})^G$ *is trivial for all $i \geq 1$.*

*Proof.* The homomorphism $G^{(i+1)}/G^{(i+2)} \to G^{(i)}/G^{(i+1)}$ induced by the inclusion map $G^{(i+1)} \hookrightarrow G^{(i)}$ is trivial. Now use Proposition 5.2 with $G_1 = G_2 = G$ , $R_1 = G^{(i+1)}$, and $R_2 = G^{(i)}$. □

The next proposition is a variant of [Bog92, Lemma 3.3].

**Lemma 5.5.** *The inflation maps*

$$\inf_{G^{[3]}}\colon H^2(G^{[2]}) \to H^2(G^{[3]}), \quad \inf_G\colon H^2(G^{[2]}) \to H^2(G)$$

*have the same kernel.*

*Proof.* The functoriality of the 5-term sequence (see §2 and [EM07, §2B)]) gives a commutative diagram with exact rows

$$\begin{array}{ccccc} H^1(G^{(2)})^G & \xrightarrow{\mathrm{trg}_{G^{[2]}}} & H^2(G^{[2]}) & \xrightarrow{\inf_G} & H^2(G) \\ \downarrow{\scriptstyle \mathrm{res}_{G^{(3)}}} & & \downarrow{\scriptstyle \inf_{G^{[3]}}} & & \| \\ H^1(G^{(3)})^G & \xrightarrow{\mathrm{trg}_{G^{[3]}}} & H^2(G^{[3]}) & \xrightarrow{\inf_G} & H^2(G). \end{array}$$

By Lemma 5.4, $\mathrm{res}_{G^{(3)}} = 0$, and the assertion follows by a diagram chase. □

**Proposition 5.6.** *Let $\pi\colon G_1 \to G_2$ be a homomorphism of profinite groups with $\pi_1^*$ bijective and $\pi_2^*$ injective. Then $\pi^{[3]}$ is an isomorphism.*

*Proof.* By Lemma 5.3, the maps $\pi^{[2]}\colon G_1^{[2]} \to G_2^{[2]}$ and $\inf_{G_i}\colon H^1(G_i^{[2]}) \to H^1(G_i)$, $i = 1, 2$, are isomorphisms. By the functoriality of the 5-term sequence, there is a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G_2^{(2)})^{G_2} & \xrightarrow{\mathrm{trg}} & H^2(G_2^{[2]}) & \xrightarrow{\inf_{G_2}} & H^2(G_2) \\ & & \downarrow{\scriptstyle (\pi^{(2)})_1^*} & & \downarrow{\scriptstyle (\pi^{[2]})_2^*} & & \downarrow{\scriptstyle \pi_2^*} \\ 0 & \longrightarrow & H^1(G_1^{(2)})^{G_1} & \xrightarrow{\mathrm{trg}} & H^2(G_1^{[2]}) & \xrightarrow{\inf_{G_1}} & H^2(G_1). \end{array}$$

Now since $\pi^{[2]}$ is an isomorphism, so is $(\pi^{[2]})_2^*$. By assumption, $\pi_2^*$ is injective. A snake lemma argument shows that $(\pi^{(2)})_1^*$ is an isomorphism. By passing to duals (using Proposition 5.2 with $R_i = G_i^{(2)}$), we obtain that the map $\bar\pi\colon G_1^{(2)}/G_1^{(3)} \to G_2^{(2)}/G_2^{(3)}$

induced by $\pi$ is also an isomorphism. Thus in the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_1^{(2)}/G_1^{(3)} & \longrightarrow & G_1^{[3]} & \longrightarrow & G_1^{[2]} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \bar\pi} & & \downarrow{\scriptstyle \pi^{[3]}} & & \downarrow{\scriptstyle \pi^{[2]}} & & \\ 1 & \longrightarrow & G_2^{(2)}/G_2^{(3)} & \longrightarrow & G_2^{[3]} & \longrightarrow & G_2^{[2]} & \longrightarrow & 1 \end{array}$$

both $\bar\pi$ and $\pi^{[2]}$ are isomorphisms. By the snake lemma, so is $\pi^{[3]}$. □

## 6. Morphisms of cohomology rings

We will now use the general constructions of §3 with the base ring $R = \mathbb{Z}/q$.

**Lemma 6.1.** *Let $\pi\colon G_1 \to G_2$ be a homomorphism of profinite groups such that $\widehat{\pi^*}$ is an isomorphism and $H^*(G_1)$ is quadratic. Then $\pi^*_{\rm dec}$ is an isomorphism and $H^*(G_2)$ is also quadratic.*

*Proof.* By (3.1), there is a commutative square

$$\begin{array}{ccc} \widehat{H^*(G_2)} & \xrightarrow{\widehat{\pi^*}} & \widehat{H^*(G_1)} \\ \downarrow{\scriptstyle \omega_{H^*(G_2)}} & & \downarrow{\scriptstyle \omega_{H^*(G_1)}} \\ H^*(G_2)_{\rm dec} & \xrightarrow{\pi^*_{\rm dec}} & H^*(G_1)_{\rm dec}. \end{array}$$

Now use the surjectivity of $\omega_{H^*(G_2)}$ and the assumptions. □

**Proposition 6.2.** *Let $\pi\colon G_1 \to G_2$ be a homomorphism of profinite groups such that $\pi^{[3]}$ is an isomorphism. Then:*

(a) *$\pi^*_{{\rm dec},2}\colon H^2(G_2)_{\rm dec} \to H^2(G_1)_{\rm dec}$ is an isomorphism;*

(b) *$\widehat{\pi^*}\colon \widehat{H^*(G_2)} \to \widehat{H^*(G_1)}$ is an isomorphism.*

*Proof.* First note that by Lemma 4.2, $\pi^{[2]}$ is also an isomorphism.

(a) One has a commutative diagram with isomorphisms as indicated:

$$\begin{array}{ccccc} H^2(G_2^{[2]})_{\rm dec} & \xrightarrow{\rm inf} & H^2(G_2^{[3]})_{\rm dec} & \xrightarrow{\rm inf} & H^2(G_2)_{\rm dec} \\ \wr\downarrow{\scriptstyle (\pi^{[2]})^*_{{\rm dec},2}} & & \wr\downarrow{\scriptstyle (\pi^{[3]})^*_{{\rm dec},2}} & & \downarrow{\scriptstyle \pi^*_{{\rm dec},2}} \\ H^2(G_1^{[2]})_{\rm dec} & \xrightarrow{\rm inf} & H^2(G_1^{[3]})_{\rm dec} & \xrightarrow{\rm inf} & H^2(G_1)_{\rm dec}. \end{array}$$

Further, by Lemma 5.3, ${\rm inf}_{G_i}\colon H^2(G_i^{[2]})_{\rm dec} \to H^2(G_i)_{\rm dec}$ is surjective for $i = 1, 2$. The assertion now follows using Lemma 5.5 (for $G = G_1$).

(b) By Lemma 5.3, $\pi_1^*\colon H^1(G_2) \to H^1(G_1)$ is an isomorphism. Now use (a) and Lemma 3.1. □

Combining the previous results we obtain:

**Theorem 6.3.** *Let $\pi\colon G_1 \to G_2$ be a homomorphism of profinite groups with $H^*(G_1)$ quadratic and $H^2(G_2)$ decomposable. The following conditions are equivalent:*

(a) *$\pi_1^*$ is bijective and $\pi_2^*$ is injective;*

(b) $\pi^{[3]}$ *is an isomorphism;*
(c) $\widehat{\pi^*}$ *is an isomorphism;*
(d) $\pi^*_{\mathrm{dec}}$ *is an isomorphism.*

*Proof.* (a)⇒(b) is Proposition 5.6. (b)⇒(c) is Proposition 6.2(b). For (c)⇒(d) use Lemma 6.1. Finally, (d)⇒(a) follows from the decomposability of $H^2(G_2)$. □

Denote the maximal pro-$p$ quotient of $G$ by $G(p)$.

**Lemma 6.4.** $\mathrm{inf}_G\colon H^2(G(p)) \to H^2(G)$ *is injective.*

*Proof.* The kernel $N$ of the epimorphism $G \to G(p)$ satisfies $H^1(N)^G = 0$. Now use the 5-term sequence. □

**Theorem 6.5.** *Let $G$ be a profinite group with $H^*(G)$ quadratic. Let $N$ be a normal subgroup of $G$ with $N \le G^{(3)}$. Then*

(a) $\mathrm{inf}_G\colon H^*(G/N)_{\mathrm{dec}} \to H^*(G)_{\mathrm{dec}}$ *is an isomorphism.*
(b) $H^*(G/N)$ *is quadratic.*
(c) *If $H^2(G/N)$ is decomposable, then $N$ is contained in the kernel of the canonical map $G \to G(p)$.*

*Proof.* Consider the natural epimorphism $\pi\colon G \to G/N$. By Lemma 4.3, $\pi^{[3]}$ is an isomorphism. By Proposition 6.2(b), $\widehat{\pi^*}$ is also an isomorphism. Assertions (a) and (b) now follow from Lemma 6.1.

To prove (c), let $M$ be the kernel of the projection $G \to G(p)$ and set $R = MN$. A standard group-theoretic argument shows that $H^1(M) = 0$. Since $H^1(R/N) \cong H^1(M/M \cap N)$ injects into it by inflation, it is also trivial. By the 5-term sequence, $\mathrm{res}_N\colon H^1(R) \to H^1(N)$ is therefore injective.

By (a), $\mathrm{inf}_G\colon H^2(G/N) = H^2(G/N)_{\mathrm{dec}} \to H^2(G)_{\mathrm{dec}}$ is an isomorphism. Also, since $N, M \le G^{(2)}$, the inflation maps $H^1(G/R) \to H^1(G)$, $H^1(G/N) \to H^1(G)$ are isomorphisms (Lemma 5.3). Using as before the functoriality of the 5-term sequence, we get a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1(R)^G & \xrightarrow{\mathrm{trg}_{G/R}} & H^2(G/R) & \xrightarrow{\mathrm{inf}_G} & H^2(G) \\
 & & \Big\downarrow{\scriptstyle \mathrm{res}_N} & & \Big\downarrow{\scriptstyle \mathrm{inf}_{G/N}} & & \Big\uparrow \\
0 & \longrightarrow & H^1(N)^G & \xrightarrow{\mathrm{trg}_{G/N}} & H^2(G/N) & \xrightarrow[\sim]{\mathrm{inf}_G} & H^2(G)_{\mathrm{dec}}
\end{array}$$

Consequently, $H^1(R)^G = 0$, whence $H^1(R/M, \mathbb{Z}/p)^{G(p)} = 0$. Since $G(p)$ is pro-$p$, it follows as in [Ser65, Lemma 2] that $R/M = 1$, i.e., $N \le M$. □

## 7. Cohomology determines $G^{[3]}$

Let $G$ be a profinite group, $S$ a free pro-$p$ group, and $\pi\colon S \to G(p)$ an epimorphism. Let $\varphi\colon G(p) \to G^{[2]}$ be the natural map and set $R = \mathrm{Ker}(\pi)$ and $T = \mathrm{Ker}(\varphi \circ \pi)$. One has a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
1 & \longrightarrow & R & \longrightarrow & S & \xrightarrow{\pi} & G(p) & \longrightarrow & 1 \\
 & & \Big\downarrow & & \Big\| & & \Big\downarrow{\scriptstyle \varphi} & & \\
1 & \longrightarrow & T & \longrightarrow & S & \longrightarrow & G^{[2]} & \longrightarrow & 1.
\end{array}$$

As $H^2(S)=0$, the corresponding 5-term sequences give as before a commutative diagram with exact rows

$$(7.1)\qquad \begin{array}{ccccccccc} 0 & \longrightarrow & H^1(S)/H^1(G(p)) & \longrightarrow & H^1(R)^S & \xrightarrow{\mathrm{trg}} & H^2(G(p)) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow{\scriptstyle \mathrm{res}_R} & & \uparrow{\scriptstyle \inf_G} & & \\ 0 & \longrightarrow & H^1(S)/H^1(G^{[2]}) & \longrightarrow & H^1(T)^S & \xrightarrow{\mathrm{trg}} & H^2(G^{[2]}) & \longrightarrow & 0. \end{array}$$

Proposition 5.1 gives a commutative diagram of perfect pairings

$$(7.2)\qquad \begin{array}{ccccc} R/R^q[R,S] & \times & H^1(R)^S & \longrightarrow & \mathbb{Z}/q \\ {\scriptstyle \iota}\downarrow & & \uparrow{\scriptstyle \mathrm{res}_R} & & \| \\ T/T^q[T,S] & \times & H^1(T)^S & \longrightarrow & \mathbb{Z}/q. \end{array}$$

**Theorem 7.1.** *The following conditions are equivalent:*

(a) $\inf_G\colon H^2(G^{[2]})\to H^2(G(p))$ *is surjective;*
(b) $\mathrm{res}_R\colon H^1(T)^S\to H^1(R)^S$ *is surjective;*
(c) $R/R^q[R,S]\to T/T^q[T,S]$ *is injective;*
(d) $R^q[R,S]=R\cap T^q[T,S]$.

*Proof.* (a)$\Leftrightarrow$(b): Apply the snake lemma to (7.1) to obtain that $\mathrm{Coker}(\mathrm{res}_R)\cong\mathrm{Coker}(\inf_G)$, and the equivalence follows.

(b)$\Leftrightarrow$(c): Use (7.2).

(c)$\Leftrightarrow$(d): The homomorphism in (c) breaks as

$$R/R^q[R,S]\to R/(R\cap T^q[T,S])\to T/T^q[T,S],$$

where the right map is injective. Therefore the injectivity of the composed map is equivalent to that of the left map, i.e., to (d). ☐

Of special importance is the case where the presentation $1\to R\to S\xrightarrow{\pi} G\to 1$ is **minimal**, i.e., $R\le S^{(2)}$. Then $\pi^{[2]}$ is an isomorphism, by Lemma 4.4. Since $\varphi^{[2]}$ is always an isomorphism, $T=S^{(2)}$, so $T^q[T,S]=S^{(3)}$. In this case, and assuming further that $q=2$, the equivalences of Theorem 7.1 were obtained in [GM97, Th. 2] and [MSp96, §5].

**Remark 7.2.** By Lemma 5.3, $\inf_G\colon H^2(G^{[2]})_{\mathrm{dec}}\to H^2(G(p))_{\mathrm{dec}}$ is surjective. Thus, if $H^2(G(p))$ is decomposable, then condition (a), whence all other conditions of Theorem 7.1, are satisfied. This was earlier observed by T. Würfel [Wür85, Prop. 8] for condition (d), in the case of minimal presentations and the descending (0-) central sequence, and under the additional assumption that the maximal abelian quotient $G_{\mathrm{ab}}$ is torsion-free.

Next let $f$ be the composed homomorphism

$$H^1(T)^S \xrightarrow{\mathrm{trg}} H^2(G^{[2]}) \xrightarrow{\inf_{G(p)}} H^2(G(p)) \xrightarrow{\inf_G} H^2(G)\ .$$

Let $\mathrm{Ker}(f)^\vee$ be the dual of $\mathrm{Ker}(f)$ in $T/T^q[T,S]$ with respect to the pairing in (7.2).

**Proposition 7.3.** *Assume that the presentation* $1\to R\to S\to G\to 1$ *is minimal. Then* $G^{[3]}\cong S^{[3]}/\mathrm{Ker}(f)^\vee$.

*Proof.* Since $R \leq S^{(2)} = T$, Proposition 5.1 shows that the restrictions $H^1(S) \to H^1(R)^S$ and $H^1(S) \to H^1(T)^S$ are the zero maps. Hence the transgression maps in (7.1) are isomorphisms. By the injectivity of $\mathrm{inf}_G\colon H^1(G(p)) \to H^1(G)$ (Lemma 6.4), $\mathrm{Ker}(f) = \mathrm{Ker}(\mathrm{res}_R)$. Therefore, by (7.2),

$$\mathrm{Ker}(f)^\vee = \mathrm{Ker}(\mathrm{res}_R)^\vee = \mathrm{Im}(\iota) = RS^{(3)}/S^{(3)}.$$

In view of Lemma 4.4, $RS^{(3)}/S^{(3)}$ is the kernel of the induced map $S^{[3]} \to (S/R)^{[3]} \cong G(p)^{[3]} = G^{[3]}$. Consequently, $S^{[3]}/\mathrm{Ker}(f)^\vee \cong G^{[3]}$. □

**Remark 7.4.** Assume that the profinite group $G$ satisfies

($*$) $G^{[2]} \cong (\mathbb{Z}/q)^I$ for some set $I$.

Then one can find $S$ and $\pi$ as above such that the presentation is minimal. Namely, take a free pro-$p$ group $S$ such that $S^{[2]} \cong G^{[2]}$. This lifts to a homomorphism $S \to G$, which is surjective, by a Frattini argument.

We further claim that under assumption ($*$), $f$ is determined by $H^r(G)$, $r = 1, 2$, the cup product $\cup\colon H^1(G) \otimes_{\mathbb{Z}} H^1(G) \to H^2(G)$ and the Bockstein map $\beta\colon H^1(G) \to H^2(G)$. Indeed, $H^1(G)$ determines $G^{[2]}$ which is its Pontrjagin dual. Set

$$\Omega(G) = (H^1(G) \otimes_{\mathbb{Z}} H^1(G)) \oplus H^1(G)$$

and consider the homomorphism

$$\Lambda_G\colon \Omega(G) \to H^2(G), \quad (\alpha_1, \alpha_2) \mapsto \cup\alpha_1 + \beta(\alpha_2).$$

Then $\Lambda\colon \Omega \to H^2$ is a natural transformation of contravariant functors. For $\bar{G} \cong (\mathbb{Z}/q)^I$, the map $\Lambda_{\bar{G}}$ is surjective, by [EM07, Cor. 2.11] (when $\bar{G}$ is not finitely generated apply a limit argument, as in [EM07, Lemma 4.1]). Now the canonical map $G \to G^{[2]}$ induces a commutative square

$$\begin{array}{ccc} \Omega(G^{[2]}) & \xrightarrow{\sim} & \Omega(G) \\ \downarrow{\scriptstyle \Lambda_{G^{[2]}}} & & \downarrow{\scriptstyle \Lambda_G} \\ H^2(G^{[2]}) & \xrightarrow{\mathrm{inf}_G} & H^2(G). \end{array}$$

From the surjectivity of $\Lambda_{G^{[2]}}$ we see that $\mathrm{inf}_G$ is determined by $\Lambda_G$ (modulo the identification $H^1(G^{[2]}) \cong H^1(G)$). Hence $\mathrm{inf}_G$ is determined by $H^1(G)$, $H^2(G)$, $\cup$ and $\beta$. Also, $S$ is determined by $H^1(G)$ only.

## 8. Absolute Galois groups

Let $F$ be a field of characteristic $\neq p$ (containing as always the group $\mu_q$ of $q$th roots of unity). By fixing a primitive $q$th root of unity we may identify $\mu_q = \mathbb{Z}/q$ as $G_F$-modules. Let $K_*^M(F)$ be again the Milnor $K$-ring of $F$ [Mil70]. Define graded $\mathbb{Z}/q$-algebras $\mathcal{A} = K_*^M(F)/q$ and $\mathcal{B} = H^*(G_F)$. Observe that they are graded-commutative and $\mathcal{A} = \mathcal{A}_{\mathrm{dec}} = \hat{\mathcal{A}}$. It can be shown that the Kummer isomorphism $F^\times/(F^\times)^q \cong H^1(G_F)$, $a(F^\times)^q \mapsto (a)_F$, extends to an epimorphism $h_F\colon \mathcal{A} \to \mathcal{B}_{\mathrm{dec}}$, called the **Galois symbol epimorphism** [GS06, §4.6]. It is bijective in degrees 1 and 2, by the Kummer isomorphism and the injectivity part of the Merkurjev–Suslin theorem, respectively [GS06]. By Lemma 3.1, $\hat{h}_F\colon \mathcal{A} = \hat{\mathcal{A}} \to \hat{\mathcal{B}}$ is an isomorphism. Furthermore, by the Rost–Voevodsky theorem ([Voe03b], [Wei09], [Wei08]), $h_F$ itself is an isomorphism and $\mathcal{B} = \mathcal{B}_{\mathrm{dec}}$. By (3.1), $\omega_{\mathcal{B}}$ is also an isomorphism, i.e., $\mathcal{B} = H^*(G_F)$ is quadratic.

Theorem 6.5(a)(b) give:

**Corollary 8.1.** *For a field $F$ as above one has:*
(a) $\inf_{G_F}\colon H^*(G_F^{[3]})_{\rm dec}\to H^*(G_F)$ *is an isomorphism;*
(b) $H^*(G_F^{[3]})$ *is quadratic.*

This establishes Theorem A, and shows that for $F$ as above, $G_F^{[3]}$ determines $H^*(G_F)$. Theorem C follows from Theorem 6.3.

Finally, the projection $F^\times/(F^\times)^q\to F^\times/(F^\times)^p$ is obviously surjective. By the Kummer isomorphism, so is the functorial map $H^1(G_F)=H^1(G_F,\mathbb{Z}/q)\to H^1(G_F,\mathbb{Z}/p)$. Consequently, $(*)$ of Remark 7.4 is satisfied for $G=G_F$. Proposition 7.3 and Remark 7.4 now give Theorem B.

**Remark 8.2.** For the maximal pro-$p$ Galois extension $F(p)$ of $F$ one has $H^1(G_{F(p)})=0$. Hence $H^*(G_{F(p)})=H^*(G_{F(p)})_{\rm dec}$ vanishes in positive degrees. A spectral sequence argument therefore shows that Lyndon–Hochschild–Serre spectral sequence corresponding to $G_F\to G_F(p)$ collapses at $E_2$, giving an isomorphism $\inf\colon H^*(G_F(p))\to H^*(G_F)$ [NSW08, Lemma 2.1.2]. Therefore in the previous discussion and in Theorems A–C we may replace $G_F$ by $G_F(p)$. In particular, $H^*(G_F(p))$ is decomposable.

By Remarks 7.2 and 8.2, the equivalent conditions of Theorem 7.1 are satisfied for $G_F$. We therefore get:

**Theorem 8.3.** *Let $1\to R\to S\to G_F(p)\to 1$ be a minimal presentation of $G_F(p)$ using generators and relations, where $S$ is a free pro-$p$ group. Then $R^q[R,S]=R\cap S^{(3)}$.*

Moreover, by Theorem 6.5(c), $G_F(p)$ has the following minimality property with respect to decomposability of $H^2$. Here $F^{(3)}$ is the fixed field of $G_F^{(3)}$ in $F_{\rm sep}$.

**Theorem 8.4.** *Suppose that $K$ is a Galois extension of $F$ containing $F^{(3)}$. Assume that $H^2(\mathrm{Gal}(K/F))$ is decomposable. Then $K\supseteq F(p)$.*

This can be viewed as a cohomological characterization of the extension $F(p)/F$.

## 9. Groups which are not maximal pro-$p$ Galois groups

We now apply Theorem A to give examples of pro-$p$ groups which cannot be realized as maximal pro-$p$ Galois groups of fields (assumed as before to contain a root of unity of order $p$). Our groups also cannot be realized as the *absolute* Galois group $G_F$ of any field $F$. Indeed, assume this were the case. When char $F=p$, the maximal pro-$p$ Galois group of $F$ is a free pro-$p$ group [NSW08, Th. 6.1.4], whereas our groups are not free. When char $F\neq p$, as $G_F$ is pro-$p$, necessarily $\mu_p\subseteq F$, and we get again a contradiction.

The groups we construct are only a sample of the most simple and straightforward examples illustrating our theorems, and many other more complicated examples can be constructed along the same lines.

Throughout this section $q=p$. We have the following immediate consequence of the analog of Theorem A for maximal pro-$p$ Galois groups (Remark 8.2):

**Proposition 9.1.** *If $G_1,G_2$ are pro-$p$ groups such that $G_1^{[3,p]}\cong G_2^{[3,p]}$ and $H^*(G_1)\not\cong H^*(G_2)$, then at most one of them can be realized as the maximal pro-$p$ Galois group of a field.*

**Corollary 9.2.** *Let $S$ be a free pro-$p$ group and $R$ a nontrivial closed normal subgroup of $S^{(3,p)}$. Then $G = S/R$ cannot occur as a maximal pro-$p$ Galois group of a field.*

*Proof.* Since $R \leq S^{(3,p)} \leq S^{(2,p)}$, there is an induced isomorphism $S^{[2,p]} \cong G^{[2,p]}$. Hence $\mathrm{inf}\colon H^1(G) \to H^1(S)$ is an isomorphism. As $H^2(S) = 0$ [NSW08, Cor. 3.9.5], $\mathrm{trg}\colon H^1(R)^G \to H^2(G)$ is also an isomorphism. Furthermore, $H^1(R) \neq 0$, so a standard orbit counting argument shows that $H^1(R)^S \neq 0$. Hence $H^2(G) \neq 0$. Now $S \cong G_F$ for some field $F$ of characteristic 0 [FJ05, Cor. 23.1.2], so we may apply Proposition 9.1 with $G_1 = S$ and $G_2 = G$. □

**Example 9.3.** Let $S$ be a free pro-$p$ group on 2 generators, and take $R = [S, [S, S]]$. By Corollary 9.2, $G = S/R$ is not realizable as $G_F(p)$ for a field $F$ as above. Note that $G/[G, G] \cong S/[S, S] \cong \mathbb{Z}_p^2$ and $[G, G] = [S, S]/S^{(3,0)} \cong \mathbb{Z}_p$ (Proposition 4.5), so $G$ is torsion-free.

**Example 9.4.** Let $S$ be a free pro-$p$ group on $n \geq 3$ generators $\sigma_1, \ldots, \sigma_n$, and let $R$ be the closed normal subgroup of $S$ generated by $r = [\ldots[[\sigma_1, \sigma_2], \sigma_3], \ldots, \sigma_n]$. By Corollary 9.2, $G = S/R$ is not realizable as $G_F(p)$ for a field $F$ as above. By Proposition 4.5, $r \notin (S^{(n,0)})^p S^{(n+1,0)}$. Therefore [Lab67, Th. 4] implies that $G = S/R$ is torsion-free. We further note that, by [Rom86], $G$ contains a subgroup which is a free pro-$p$ group on two generators. In particular, $G$ is not prosolvable.

**Example 9.5.** Let $S$ be a free pro-$p$ group on generators $\sigma_1, \sigma_2$. Let $r_1 = \sigma_1^p$ and $r_2 = \sigma_1^p[\sigma_1, [\sigma_1, \sigma_2]]$. Let $R_i$ be the normal subgroup of $S$ generated by $r_i$, and set $G_i = S/R_i$, $i = 1, 2$. As $r_1 r_2^{-1} \in S^{[3,p]}$ we have $G_1^{[3,p]} \cong G_2^{[3,p]}$.

Since $G_1$ has $p$-torsion, it has $p$-cohomological dimension $\mathrm{cd}_p(G_1) = \infty$ [Ser02, I, §3.3, Cor. 3]. On the other hand, $\mathrm{cd}_p(G_2) = 2$; indeed, this is proved in [Lab67, p. 144, Example (1)] for $p \geq 5$, in [Lab67, p. 157, Exemple] for $p = 3$, and in [Gil68, Prop. 3] for $p = 2$. By [Ser02, I, §3.3, Cor. 3] again, $G_2$ is torsion-free. Furthermore, $H^*(G_1) \ncong H^*(G_2)$.

Now if $p = 2$, then $G_1$ is the free pro-2 product $(\mathbb{Z}/2) * \mathbb{Z}_2$, which is an absolute Galois group of a field, e.g., an algebraic extension of $\mathbb{Q}$ [Efr99]. By Proposition 9.1, $G_2$ is not a maximal pro-$p$ Galois group.

Finally, for $p > 2$, [BLMS07, Th. A.3] or [EM07, Prop. 12.3] imply that in this case as well, $G_2$ is not a maximal pro-$p$ Galois group.

**Proposition 9.6.** *Let $G$ be a pro-$p$ group such that $\dim_{\mathbb{F}_p} H^1(G) < \mathrm{cd}(G)$. When $p = 2$ assume also that $G$ is torsion-free. Then $G$ is not a maximal pro-$p$ Galois group of a field as above.*

*Proof.* Assume that $p \neq 2$. Let $d = \dim_{\mathbb{F}_p} H^1(G)$. Then also $d = \dim_{\mathbb{F}_p} H^1(G^{[3,p]})$. Since the cup product is graded-commutative, $H^{d+1}(G^{[3,p]})_{\mathrm{dec}} = 0$. On the other hand, $H^{d+1}(G) \neq 0$ [NSW08, Prop. 3.3.2]. Thus $H^*(G^{[3,p]})_{\mathrm{dec}} \ncong H^*(G)$. By Theorem A and Remark 8.2, $G$ is not a maximal pro-$p$ Galois group.

When $p = 2$ this was shown in [AKM99, Th. 3.21], using Kneser's theorem on the $u$-invariant of quadratic forms, and a little later (independently) by R. Ware in a letter to the third author. □

**Example 9.7.** Let $K, L$ be finitely generated pro-$p$ groups with $1 \leq n = \mathrm{cd}(K) < \infty$, $\mathrm{cd}(L) < \infty$, and $H^n(K)$ finite. Let $\pi\colon L \to \mathrm{Sym}_m$, $x \mapsto \pi_x$, be a homomorphism such that $\pi(L)$ is a transitive subgroup of $\mathrm{Sym}_m$. Then $L$ acts on $K^m$ from the left by ${}^x(y_1,\dots,y_m)=(y_{\pi_x(1)},\dots,y_{\pi_x(m)})$. Let $G=K^m\rtimes L$. It is generated by the generators of one copy of $K$ and of $L$. Hence $\dim_{\mathbb{F}_p}H^1(G)=\dim_{\mathbb{F}_p}H^1(K)+\dim_{\mathbb{F}_p}H^1(L)$.

On the other hand, a routine inductive spectral sequence argument (see [NSW08, Prop. 3.3.8]) shows that for every $i\geq 0$ one has

(1) $\mathrm{cd}(K^i)=in$;
(2) $H^{in}(K^i)=H^n(K,H^{(i-1)n}(K^{i-1}))$, with the trivial $K$-action, is finite.

Moreover, $\mathrm{cd}(G)=\mathrm{cd}(K^m)+\mathrm{cd}(L)$. For $m$ sufficiently large we get $\dim_{\mathbb{F}_p}H^1(G)<mn+\mathrm{cd}(L)=\mathrm{cd}(G)$, so by Proposition 9.6, $G$ is not a maximal pro-$p$ Galois group as above. When $K,L$ are torsion-free, so is $G$.

For instance, one can take $K$ to be a free pro-$p$ group $\neq 1$ on finitely many generators, and let $L=\mathbb{Z}_p$ act on the direct product of $p^s$ copies of $K$ via $\mathbb{Z}_p\to\mathbb{Z}/p^s$ by cyclicly permuting the coordinates.

**Remark 9.8.** Absolute Galois groups which are solvable (with respect to closed subgroups) were analyzed in [Gey69], [Bec78], [Wür85, Cor. 1], [Koe01]. In particular one can give examples of such solvable groups which are not absolute Galois groups (compare [Koe01, Example 4.9]). Our examples here are in general not solvable.

## References


[AKM99] A. Adem, D. B. Karagueuzian, and J. Mináč, *On the cohomology of Galois groups determined by Witt rings*, Adv. Math. **148** (1999), 105–160.

[Bec74] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, J. reine angew. Math. **268/269** (1974), 41–52.

[Bec78] E. Becker, *Formal-reelle Körper mit streng-auflösbarer absoluter Galoisgruppe*, Math. Ann. **238** (1978), 203–206.

[BLMS07] D. J. Benson, N. Lemire, J. Mináč, and J. Swallow, *Detecting pro-p-groups that are not absolute Galois groups*, J. reine angew. Math. **613** (2007), 175–191.

[Bog91] F. A. Bogomolov, *On two conjectures in birational algebraic geometry*, Proc. of Tokyo Satellite conference ICM-90 Analytic and Algebraic Geometry, 1991, pp. 26–52.

[Bog92] F. A. Bogomolov, *Abelian subgroups of Galois groups*, Math. USSR, Izv. **38** (1992), 27–67 (English; Russian original).

[BT08] F. Bogomolov and Y. Tschinkel, *Reconstruction of function fields*, Geom. Func. Anal. **18** (2008), 400-462.

[BT09] F. A. Bogomolov and Y. Tschinkel, *Milnor $K_2$ and field homomorphisms* (2009), preprint.

[Efr99] I. Efrat, *Finitely generated pro-p absolute Galois groups over global fields*, J. Number Theory **77** (1999).

[EM07] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups* (2007), to appear.

[FJ05] M. D. Fried and M. Jarden, *Field Arithmetic*, 2nd ed., Springer-Verlag, Berlin, 2005.

[GM97] W. Gao and J. Mináč, *Milnor's conjecture and Galois theory I*, Fields Institute Communications **16** (1997), 95–110.

[Gey69] W.-D. Geyer, *Unendliche Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist*, J. Number Theory **1** (1969), 346–374.

[GS06] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge University Press, Cambridge, 2006.

[Gil68] D. Gildenhuys, *On pro-p groups with a single defining relator*, Inv. math. **5** (1968), 357–366.

[HW09] C. Haesemeyer and C. Weibel, *Norm Varieties and the Chain Lemma (after Markus Rost)*, Proc. Abel Symposium **4** (2009), to appear.

[Koc02] H. Koch, *Galois theory of p-extensions*, Springer-Verlag, Berlin, 2002.

[Koe01] J. Koenigsmann, *Solvable absolute Galois groups are metabelian*, Inv. math. **144** (2001), 1–22.

[Lab66] J. P. Labute, *Demuškin groups of rank* $\aleph_0$, Bull. Soc. Math. France **94** (1966), 211–244.

[Lab67] J. P. Labute, *Algèbres de Lie et pro-p-groupes définis par une seule relation*, Inv. math. **4** (1967), 142–158.

[MMS04] L. Mahé, J. Mináč, and T. L. Smith, *Additive structure of multiplicative subgroups of fields and Galois theory*, Doc. Math. **9** (2004), 301-355.

[MS82] 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), 1011–1046 (Russian); English transl., Math. USSR Izv. **21** (1983), 307–340.

[Mil70] J. Milnor, *Algebraic K-theory and quadratic forms*, Invent. Math. **9** (1969/1970), 318–344.

[MSp90] J. Mináč and M. Spira, *Formally real fields, Pythagorean fields, C-fields and W-groups*, Math. Z. **205** (1990), 519–530.

[MSp96] J. Mináč and M. Spira, *Witt rings and Galois groups*, Ann. of Math. (2) **144** (1996), 35–60.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields, Second edition*, Springer, Berlin, 2008.

[OVV07] D. Orlov, A. Vishik, and V. Voevodsky, *An exact sequence for* $K_*^M/2$ *with applications to quadratic forms*, Ann. Math. **165** (2007), 1–13.

[Rom86] N. S. Romanovskij, *Generalized theorem on the freedom for pro-p-groups*, Sib. Mat. Zh. **156** (1986), 154–170.

[Ser65] J.-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology **3** (1965), 413–420.

[Ser02] J.-P. Serre, *Galois cohomology*, Springer, Berlin, 2002. Translated from the 1964 French Edition by Patrick Ion and revised by the author.

[Spi87] M. Spira, *Witt rings and Galois groups*, Ph.D. thesis, University of California, Berkeley, 1987.

[Voe03a] V. Voevodsky, *Motivic cohomology with* $\mathbb{Z}/2$*-coefficients*, Publ. Math. Inst. Hautes Études Sci. **98** (2003), 59–104.

[Voe03b] V. Voevodsky, *On motivic cohomology with* $\mathbb{Z}/l$*-coefficients* (2003), available at `http://www.math.uiuc.edu/K-theory/0639/`. revised in 2009.

[Wei08] C. A. Weibel, *The proof of the Bloch–Kato conjecture*, ICTP Lecture Notes series **23** (2008), 1–28.

[Wei09] C. A. Weibel, *The norm residue isomorphism theorem* (2009), available at `http://www.math.uiuc.edu/K-theory/0934/`. to appear in J. Topology.

[Wür85] T. Würfel, *On a class of pro-p groups occurring in Galois theory*, J. Pure Appl. Algebra **36** (1985), 95–103.

Department of Mathematics, Illinois State University, Campus box 4520, Normal, IL 61790, USA

*E-mail address*: `schebol@ilstu.edu`

Mathematics Department, Ben-Gurion University of the Negev, P.O. Box 653, Be'er-Sheva 84105, Israel

*E-mail address*: `efrat@math.bgu.ac.il`

Mathematics Department, University of Western Ontario, London, Ontario, Canada N6A 5B7

*E-mail address*: `minac@uwo.ca`