ON THE DESCENDING CENTRAL SEQUENCE OF ABSOLUTE GALOIS GROUPS

IDO EFRAT AND JÁN MINÁČ

Abstract. Let p be an odd prime number and F a field containing a primitive pth root of unity. We prove a new restriction on the group-theoretic structure of the absolute Galois group G_F of F. Namely, the third subgroup $G_F^{(3)}$ in the descending p-central sequence of G_F is the intersection of all open normal subgroups N such that G_F/N is 1, $\mathbb{Z}/p^2$, or the extra-special group M_{p^3} of order p^3 and exponent p^2.

1. Introduction

Let $q = p^d$ be a prime power and let G be a profinite group. The **descending q-central sequence** of G is defined inductively by

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

Thus $G^{(i+1)}$ is the closed subgroup of G generated by all powers h^q and all commutators $[h, g] = h^{-1}g^{-1}hg$, where $h \in G^{(i)}$ and $g \in G$.

Now suppose that $q = p$. Let F be a field containing a primitive pth root of unity ζ_p, and let $G = G_F$ be its absolute Galois group. Let M_{p^3} be the unique nonabelian group of order p^3 and exponent p^2 (see §8).

Main Theorem. *For $p \neq 2$ and for $G = G_F$ as above, $G^{(3)}$ is the intersection of all open normal subgroups N of G such that G/N is isomorphic to one of 1, $\mathbb{Z}/p^2$, and M_{p^3}.*

Determining the profinite groups which are realizable as absolute Galois groups of fields is a major open problem in Galois theory. Our Main Theorem appears to be simple yet powerful restriction on the possible structure of such groups, and on their quotients $G_F/G_F^{(3)}$. These quotients an extremely important invariant of fields, carrying a substantial information about their arithmetical structure. For example,

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

Key words and phrases. descending central sequence, absolute Galois group, Galois cohomology, embedding problem, W-group, Bockstein map.

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

when $p = 2$ it encodes the orderings and the Witt ring of quadratic forms of F ([MSp90], [MSp96]) as well as some non-trivial valuations [MMS04]. Further, it encodes the entire mod 2 Galois cohomology ring of G_F [AKM99, Th. 3.14]. In a forthcoming joint work with S. Chebolu we show that $G_F/G_F^{(3)}$ can be in fact thought of as a group-theoretic analog of Galois cohomology of F for any p, and use these results to provide new examples of profinite groups which are not realizable as absolute Galois groups of fields.

The analog of our Main Theorem for $p = 2$ was discovered by Villegas in a different formalism [Vil88]. The second author and Spira reformulated and reproved it in [MSp96, Cor. 2.18] using the descending 2-central sequence of G_F. Namely, then $G^{(3)} = G_F^{(3)}$ is the intersection of all open normal subgroups N of G such that G/N is isomorphic to 1, $\mathbb{Z}/2$, $\mathbb{Z}/4$, or to the dihedral group $D_4 = M_8$ of order 8.

A main difference between the case $p > 2$ and the case $p = 2$ is the existence in the former case of elements in $H^2((\mathbb{Z}/p)^n, \mathbb{Z}/p)$ which are not expressible as sums of cup products of elements in $H^1((\mathbb{Z}/p)^n, \mathbb{Z}/p)$. To handle this new kind of elements we study the Bockstein homomorphism $\beta_G\colon H^1(G, \mathbb{Z}/p) \to H^2(G, \mathbb{Z}/p)$ and its relation to Galois theory.

Our approach is purely cohomological. Thus we prove the Main Theorem more generally for profinite groups G which satisfy two simple conditions on their lower cohomology. These conditions are known to hold for $G = G_F$, with F as above, where they are consequences of the following two Galois-theoretic facts (see §3 for details and terminology):

(i) the Galois symbol $K_2^M(F)/p \to H^2(G, \mathbb{Z}/p)$ is injective (it is actually bijective by the Merkurjev–Suslin theorem, which is a special case of the Rost–Voevodsky's theorem); and

(ii) β_G is the cup product by the Kummer element $(\zeta_p) \in H^1(G, \mathbb{Z}/p)$.

More generally, when $q = p^d$ is an arbitrary prime power and F is a field containing a primitive qth root of unity, we characterize $G_F^{(3)}$ as the intersection of all open normal subgroups N of G_F such that G_F/N belongs to a certain cohomologically defined class of finite groups (Theorem 5.2). This is based on the natural generalizations of (i) and (ii) above, as well as the following additional property of G_F:

(iii) the map $H^1(G_F, \mathbb{Z}/q) \to H^1(G_F, \mathbb{Z}/p^i)$, $1 \leq i \leq d$, is surjective.

Our analysis applies also to $p = 2$. Thus we give a new cohomological proof of the above-mentioned result of [Vil88] and [MSp96], and generalize it to profinite groups G satisfying the appropriate conditions on their lower cohomology. We also show that the group $\mathbb{Z}/2$ can be omitted from the list unless F is a Euclidean field (Corollary 11.4).

The paper is organized as follows: In §2 we collect various cohomological preliminaries, especially facts related to the Bockstein homomorphism β_G and its connections with roots of unity and cup products. In §3 we introduce the key notion of a profinite group of Galois relation type. It axiomatizes the cohomological properties of absolute Galois groups that we need for our proofs ((i)–(iii) above). In §4 we define an abelian group $\Omega(G)$ and a homomorphism $\Lambda_G\colon \Omega(G) \to H^2(G,\mathbb{Z}/q)$. These extend the cup product $\cup\colon H^1(G,\mathbb{Z}/q)^{\otimes 2} \to H^2(G,\mathbb{Z}/q)$, but take into account also the Galois-theoretic role of β_G. Our axioms on G imply that $\mathrm{Ker}(\Lambda_G)$ is generated by elements of simple type (Definition 4.2 and Proposition 4.3). These simple type elements are in turn related to cohomologically defined open subgroups N of G of index dividing q^3, which we call "distinguished subgroups". In §5 we translate the above result about $\mathrm{Ker}(\Lambda_G)$ to the language of distinguished subgroups, and prove the crucial Theorem 5.2: for G of Galois relation type, $G^{(3)}$ is the intersection of all distinguished subgroups of G.

In §§6–10 we build a "dictionary" between the images under Λ_G of simple type elements of $\Omega(G)$ and some special group extensions. The solutions of the resulting embedding problems correspond to distinguished subgroups of G. This is then used in §11 to prove the Main Theorem and the analogous results for $p = 2$ in the general setting of profinite groups of Galois relation type.

In §12 we study $G/G^{(3)}$ for G of Galois relation type. As a corollary we recover some known "automatic realization" results in Galois theory. Our approach seems to provide a good explanation why these curious automatic realization results are true. Finally, in §13 we give examples showing that all the finite groups in our lists are indeed necessary.

We thank P. Deligne, L. Moret-Baily, A. Shalev, and T. Weigel for their interest in this work and their comments related to talks given at the Israel Mathematical Union 2008 conference and the 2008 conference on Profinite Groups in ESI, Vienna. We also thank Y. Tschinkel for his kind encouragement.

2. Cohomological preliminaries

Let p be a prime number, let $q = p^d$ be a power of p, and let G be a profinite group. We write $H^i(G)$ for the profinite cohomology group $H^i(G,\mathbb{Z}/q)$, where G acts trivially on $\mathbb{Z}/q$. Thus $H^1(G) = \mathrm{Hom}(G,\mathbb{Z}/q)$ consists of all continuous group homomorphisms $G \to \mathbb{Z}/q$. We consider $H^*(G) = \bigoplus_{i=0}^{\infty} H^i(G)$ as a graded anti-commutative ring with respect to the cup product $\cup$.

A) Normal Subgroups. Let N be a normal closed subgroup of G. Then G acts canonically on $H^i(N)$. Denote the group of all G-invariant elements of $H^i(N)$ by $H^i(N)^G$. For $i=1$ this action is given by $\varphi \mapsto \varphi^g$, where $\varphi^g(n)=\varphi(g^{-1}ng)$ for $g\in G$ and $n\in N$. Thus $H^1(N)^G$ consists of all homomorphisms $\varphi\colon N\to \mathbb{Z}/q$ which are trivial on $N^q[N,G]$.

The next lemma provides a fundamental connection between the descending q-central sequence of G and cohomology.

Lemma 2.1. *For a normal closed subgroup N of G one has*

$$\bigcap\{\mathrm{Ker}(\varphi)\mid \varphi\in H^1(N)^G\}=N^q[N,G].$$

Proof. Consider the natural projection $\pi\colon N\to \bar N=N/N^q[N,G]$. The abelian torsion group $\bar N$ has Pontryagin dual $H^1(\bar N)$. By the Pontryagin duality [NSW00, Th. 1.1.8], $\bigcap_{\bar\varphi\in H^1(\bar N)}\mathrm{Ker}(\bar\varphi)=\{0\}$, whence $\bigcap_{\bar\varphi\in H^1(\bar N)}\pi^{-1}(\mathrm{Ker}(\bar\varphi))=N^q[N,G]$. Further, if $\bar\varphi\in H^1(\bar N)$ and $\varphi=\mathrm{inf}_N(\bar\varphi)$, then $\mathrm{Ker}(\varphi)=\pi^{-1}(\mathrm{Ker}(\bar\varphi))$. Finally, by the previous remarks, $\mathrm{inf}_N\colon H^1(\bar N)\to H^1(N)^G$ is an isomorphism. The assertion follows. □

Corollary 2.2. *There is a natural non-degenerate pairing*

$$N/N^q[N,G]\times H^1(N)^G\to \mathbb{Z}/q.$$

Corollary 2.3. *$G^{(i)}/G^{(i+1)}$ is dual to $H^1(G^{(i)})^G$ for $i\geq 1$.*

B) Spectral sequences. Let N be a closed normal subgroup of G. Recall that the Hochschild–Serre spectral sequence

$$E_2^{ij}=H^i(G/N,H^j(N))\Rightarrow H^{i+j}(G)$$

induces the 5-term exact sequence

(2.1)
$$0\to H^1(G/N)\xrightarrow{\mathrm{inf}_G} H^1(G)\xrightarrow{\mathrm{res}_N} H^1(N)^G\xrightarrow{\mathrm{trg}_{G/N}} H^2(G/N)\xrightarrow{\mathrm{inf}_G} H^2(G).$$

Here $\mathrm{trg}_{G/N}$ is the differential $d_2^{0,1}$ of the spectral sequence [NSW00, §2.1]. If N' is another closed normal subgroup of G and $N'\leq N$, then the projection $G/N'\to G/N$ and the restriction map $\mathrm{res}_{N'}\colon H^j(N)\to H^j(N')$ induce a spectral sequence morphism from $H^i(G/N,H^j(N))\Rightarrow H^{i+j}(G)$ to $H^i(G/N',H^j(N'))\Rightarrow H^{i+j}(G)$ [NSW00, pp. 78–79]. In particular, there is a commutative diagram

(2.2)
$$\begin{array}{ccc} H^1(N)^G & \xrightarrow{\mathrm{trg}_{G/N}} & H^2(G/N)\\ \Big\downarrow{\scriptstyle \mathrm{res}_{N'}} & & \Big\downarrow{\scriptstyle \mathrm{inf}_{G/N'}}\\ H^1(N')^G & \xrightarrow{\mathrm{trg}_{G/N'}} & H^2(G/N'). \end{array}$$

C) Connecting homomorphisms. Let n, m be positive integers. The exact sequences

$$0 \to \mathbb{Z}/n \to \mathbb{Z}/mn \to \mathbb{Z}/m \to 0$$

$$0 \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} \hookrightarrow \tfrac{1}{mn}\mathbb{Z}/\mathbb{Z} \xrightarrow{n} \tfrac{1}{m}\mathbb{Z}/\mathbb{Z} \to 0$$

of trivial G-modules give rise to connecting homomorphisms

$$\beta_{G,m,n}\colon H^1(G, \mathbb{Z}/m) \to H^2(G, \mathbb{Z}/n)$$
$$\beta'_{G,m,n}\colon H^1(G, \tfrac{1}{m}\mathbb{Z}/\mathbb{Z}) \to H^2(G, \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}),$$

respectively. When $m = n = q$ is our fixed p-power, we abbreviate

$$\beta_G = \beta_{G,q,q}$$

and call it the **Bockstein homomorphism** of G. Note that it is functorial in G. We now relate $\beta_{G,m,n}$ to some other connecting homomorphisms and cup products.

Lemma 2.4. *Suppose $q = 2$. For $\psi \in H^1(G)$ one has $\beta_G(\psi) = \psi \cup \psi$.*

Proof. This is straightforward when $G \cong \mathbb{Z}/2$. In the general case, it follows by inflating from $G/\operatorname{Ker}(\psi)$ to G. □

Next let $\epsilon\colon H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ be the connecting map arising from the short exact sequence of trivial G-modules

$$0 \to \mathbb{Z} \hookrightarrow \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Since $\mathbb{Q}$ is cohomologically trivial, ϵ is in fact an isomorphism. Let

$$j_m\colon \tfrac{1}{m}\mathbb{Z}/\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m, \quad \pi_n\colon \mathbb{Z} \to \mathbb{Z}/n$$

be the natural maps. A routine computation gives:

Lemma 2.5. *$\beta_{G,m,n} \circ j_m^* = \pi_n^* \circ \epsilon$ on $H^1(G, \tfrac{1}{m}\mathbb{Z}/\mathbb{Z})$.*

Now let F be a field. Set $(\mathbb{Q}/\mathbb{Z})' = \bigoplus_{l \neq \mathrm{char}\, F} (\mathbb{Q}/\mathbb{Z})_l$, where for l prime $(\mathbb{Q}/\mathbb{Z})_l$ is the l-primary component of $\mathbb{Q}/\mathbb{Z}$. Assume that $\mathrm{char}\, F \nmid n, m$. For an integer r consider the r-th Tate twists $(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r)$, $(\mathbb{Z}/n)(r)$, and $(\mathbb{Q}/\mathbb{Z})'(r)$ [NSW00, Def. 7.3.6]. Let $\iota_n\colon (\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r) \xrightarrow{\sim} (\mathbb{Z}/n)(r)$ be the isomorphism of multiplication by n. Thus $\mu_n = (\mathbb{Z}/n)(1)$ is the G_F-module of nth roots of unity, and $\iota_n = j_n$ when $r = 0$. The exact sequence

$$0 \to (\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r) \hookrightarrow (\mathbb{Q}/\mathbb{Z})'(r) \xrightarrow{n} (\mathbb{Q}/\mathbb{Z})'(r) \to 0 \tag{2.3}$$

gives rise to a connecting homomorphism

$$\delta^{i,r}\colon H^i(G_F, (\mathbb{Q}/\mathbb{Z})'(r)) \to H^{i+1}(G_F, (\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r)).$$

Lemma 2.6. *There is an equality of maps*

$$\delta^{i,r}\cup \mathrm{id}=\mathrm{id}\cup\delta^{j,s}\colon H^i(G_F,(\mathbb{Q}/\mathbb{Z})'(r))\times H^j(G_F,(\mathbb{Q}/\mathbb{Z})'(s)) \to H^{i+j+1}(G_F,(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r+s)).$$

Proof. Tensorizing (2.3) with $(\mathbb{Q}/\mathbb{Z})'(s)$ gives the same sequence but with $(r+s)$-twists, which is also exact. Therefore the composed map

$$H^i(G_F,(\mathbb{Q}/\mathbb{Z})'(r))\times H^j(G_F,(\mathbb{Q}/\mathbb{Z})'(s))\xrightarrow{\cup} H^{i+j}(G_F,(\mathbb{Q}/\mathbb{Z})'(r+s)) \xrightarrow{\delta^{i+j,r+s}} H^{i+j+1}(G_F,(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r+s))$$

breaks as $\delta^{i,r}\cup\mathrm{id}$ [GS06, Prop. 3.4.8]. Similarly, it breaks also as $\mathrm{id}\cup\delta^{j,s}$, and the equality follows. ☐

For F and n as above, consider the Kummer homomorphism

$$\kappa_n\colon F^\times=H^0(G_F,F_{\mathrm{sep}}^\times)\to H^1(G_F,\mu_n).$$

Lemma 2.7. (a) $\beta'_{G_F,m,n}$ *is the restriction of* $\delta^{1,0}$ *to* $H^1(G_F,\frac{1}{m}\mathbb{Z}/\mathbb{Z})$.

(b) $\iota_n^*\circ\delta^{0,1}=\kappa_n\circ\iota_m^*$ *on* $H^0(G_F,(\frac{1}{m}\mathbb{Z}/\mathbb{Z})(1))$.

Proof. For every r there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \to & (\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r) & \hookrightarrow & (\tfrac{1}{mn}\mathbb{Z}/\mathbb{Z})(r) & \xrightarrow{n} & (\tfrac{1}{m}\mathbb{Z}/\mathbb{Z})(r) & \to & 0\\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \to & (\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r) & \hookrightarrow & (\mathbb{Q}/\mathbb{Z})'(r) & \xrightarrow{n} & (\mathbb{Q}/\mathbb{Z})'(r) & \to & 0.
\end{array}$$

It gives rise to a commutative square of connecting homomorphisms

$$\begin{array}{ccc}
H^i(G_F,(\tfrac{1}{m}\mathbb{Z}/\mathbb{Z})(r)) & \xrightarrow{\delta} & H^{i+1}(G_F,(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r))\\
\downarrow & & \|\\
H^i(G_F,(\mathbb{Q}/\mathbb{Z})'(r)) & \xrightarrow{\delta^{i,r}} & H^{i+1}(G_F,(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(r)).
\end{array}\tag{2.4}$$

For $i=1$ and $r=0$ we have $\delta=\beta'_{G_F,m,n}$, and the left vertical map in (2.4) is an embedding. This proves (a).

Next take in (2.4) $i=0$ and $r=1$ and consider the resulting connecting map δ. From the commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \to & (\tfrac{1}{n}\mathbb{Z}/\mathbb{Z})(1) & \hookrightarrow & (\tfrac{1}{mn}\mathbb{Z}/\mathbb{Z})(1) & \xrightarrow{n} & (\tfrac{1}{m}\mathbb{Z}/\mathbb{Z})(1) & \to & 0\\
 & & \wr\downarrow \iota_n & & \wr\downarrow \iota_{mn} & & \wr\downarrow \iota_m & & \\
1 & \to & \mu_n & \hookrightarrow & \mu_{mn} & \xrightarrow{n} & \mu_m & \to & 1\\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \to & \mu_n & \hookrightarrow & F_{\mathrm{sep}}^\times & \xrightarrow{n} & F_{\mathrm{sep}}^\times & \to & 1,
\end{array}$$

we get that $\iota_n^* \circ \delta = \kappa_n \circ \iota_m^*$. Combined with (2.4), this gives (b). □

Corollary 2.8. *Let* $d = \gcd(m, n)$.

(a) *There is an equality of maps*

$$\iota_d^* \circ (\beta'_{G_F,m,n} \cup \mathrm{id}) = \iota_m^* \cup (\kappa_n \circ \iota_m^*) \colon$$
$$H^1(G_F, \tfrac{1}{m}\mathbb{Z}/\mathbb{Z}) \times H^0(G_F, (\tfrac{1}{m}\mathbb{Z}/\mathbb{Z})(1)) \to H^2(G_F, \mu_d).$$

(b) *There is an equality of maps*

$$\beta_{G_F,m,n} \cup \mathrm{id} = \mathrm{id} \cup \kappa_n \colon H^1(G_F, \mathbb{Z}/m) \times H^0(G_F, \mu_m) \to H^2(G_F, \mu_d).$$

Proof. As $(\frac{1}{m}\mathbb{Z}/\mathbb{Z}) \otimes (\frac{1}{n}\mathbb{Z}/\mathbb{Z}) \cong \frac{1}{d}\mathbb{Z}/\mathbb{Z}$, Lemma 2.6 gives

$$\iota_d^* \circ (\delta^{1,0} \cup \mathrm{id}) = \iota_d^* \circ (\mathrm{id} \cup \delta^{0,1}) = \iota_m^* \cup (\iota_n^* \circ \delta^{0,1})$$

on $H^1(G_F, \frac{1}{m}\mathbb{Z}/\mathbb{Z}) \times H^0(G_F, (\frac{1}{m}\mathbb{Z}/\mathbb{Z})(1))$. By Lemma 2.7, this restricts to (a). (b) follows from (a). □

See [Led05, p. 91], [GS06, Lemma 7.5.10], and [Koc02, Th. 8.13] for related results.

D) Cohomology of finite abelian p-groups. For a profinite group G, let $H^i_{\mathrm{dec}}(G)$ be the **decomposable part** of $H^i(G)$, i.e., its subgroup generated by cup products of elements of $H^1(G)$. In this subsection we show that when $G = (\mathbb{Z}/q)^n$, the group $H^2(G)$ is generated by $H^i_{\mathrm{dec}}(G)$ and the image of β_G. In fact, for every finite abelian p-group G of exponent divisible by $q = p^d$, the structure of $H^*(G)$ as a graded ring was computed by Chapman (for $p \neq 2$) and by Townsley-Kulich (for $p = 2$), in terms of generators and relations ([Cha82], [TK88]). Since the identification of the Bockstein elements as generators is somewhat implicit in [Cha82] and [TK88], we outline an alternative proof of the required result. It is based on the following decomposition of $H^2(G)$ to its symmetric and skew-symmetric parts, as studied by Tignol and Amitsur ([TA85], [Tig86]); see also Massy [Mas87].

Let G be a finite abelian group and A be a finite trivial G-module. Call a map $a\colon G \times G \to A$ **skew-symmetric** if it is $\mathbb{Z}$-bilinear and $a(\sigma, \sigma) = 0$ for all $\sigma \in G$. Then $a(\sigma, \tau) = -a(\tau, \sigma)$ for $\sigma, \tau \in G$. The set $\mathrm{Skew}(G, A)$ of all such maps forms an abelian group under addition.

For a 2-cocycle $f \in Z^2(G, A)$ define $a_f \in \mathrm{Skew}(G, A)$ by $a_f(\sigma, \tau) = f(\sigma, \tau) - f(\tau, \sigma)$. We call f **symmetric** if $a_f = 0$. Since the action of G on A is trivial, 2-coboundries are symmetric. Let $H^2(G, A)_{\mathrm{sym}}$ be the subgroup of $H^2(G, A)$ consisting of all cohomology classes of symmetric 2-cocyles. The map $f \mapsto a_f$ induces a homomorphism Ψ with a split exact sequence [TA85, Prop. 1.3]

$$0 \to H^2(G, A)_{\mathrm{sym}} \to H^2(G, A) \xrightarrow{\Psi} \mathrm{Skew}(G, A) \to 0. \tag{2.5}$$

For ϵ as above, $\epsilon \cup \mathrm{id}$ gives by [Tig86, Prop. 1.5] an isomorphism

$$H^1(G,\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} A \xrightarrow{\sim} H^2(G,A)_{\mathrm{sym}}, \tag{2.6}$$

Now let $A = \mathbb{Z}/q$.

Proposition 2.9. *For $G = (\mathbb{Z}/q)^n$ one has $\Psi(H^2_{\mathrm{dec}}(G)) = \mathrm{Skew}(G,\mathbb{Z}/q)$.*

Proof. Write $G = \langle\sigma_1\rangle \times \cdots \times \langle\sigma_n\rangle$ with σ_i of order q. Take $\chi_1,\ldots,\chi_n \in H^1(G)$ such that $\chi_i(\sigma_i) = 1$ for all i, and $\chi_i(\sigma_k) = 0$ for $i \neq k$. For distinct i,j the cohomology class $\chi_i \cup \chi_j$ is represented by the 2-cocyle $(\sigma,\tau) \mapsto \chi_i(\sigma)\chi_j(\tau)$. Hence

$$(\Psi(\chi_i \cup \chi_j))(\sigma_k,\sigma_l) = \chi_i(\sigma_k)\chi_j(\sigma_l) - \chi_i(\sigma_l)\chi_j(\sigma_k)$$

is 1 if $(i,j) = (k,l)$, is -1 if $(i,j) = (l,k)$, and is 0 otherwise.

Now given $a \in \mathrm{Skew}(G,\mathbb{Z}/q)$, take $\varphi = \sum_{i<j} a(\sigma_i,\sigma_j)\cdot \chi_i \cup \chi_j$. For $k < l$ we get $(\Psi(\varphi))(\sigma_k,\sigma_l) = a(\sigma_k,\sigma_l)$. But maps in $\mathrm{Skew}(G,\mathbb{Z}/q)$ are determined by their values on (σ_k,σ_l), $k < l$. Hence $\Psi(\varphi) = a$. □

Proposition 2.10. *Let G be a finite abelian p-group. Then β_G maps $H^1(G)$ isomorphically onto $H^2(G)_{\mathrm{sym}}$.*

Proof. As $(\mathbb{Z}/q) \otimes_{\mathbb{Z}} (\mathbb{Z}/q) \cong \mathbb{Z}/q$, the isomorphism (2.6) coincides with

$$(\pi_q^* \circ \epsilon) \cup \mathrm{id}\colon H^1(G,\mathbb{Q}/\mathbb{Z}) \otimes H^0(G) \to H^2_{\mathrm{sym}}(G),$$

where $\pi_q\colon \mathbb{Z} \to \mathbb{Z}/q$ is the natural map. Moreover, $H^0(G) = \mathbb{Z}/q$, so

$$H^1(G,\tfrac{1}{q}\mathbb{Z}/\mathbb{Z}) \otimes H^0(G) = H^1(G,\mathbb{Q}/\mathbb{Z}) \otimes H^0(G).$$

By Lemma 2.5, (2.6) is therefore also given by

$$(\beta_G \circ j_q^*) \cup \mathrm{id}\colon H^1(G,\tfrac{1}{q}\mathbb{Z}/\mathbb{Z}) \otimes H^0(G) \to H^2_{\mathrm{sym}}(G),$$

and the latter isomorphism may be identified with β_G. □

Corollary 2.11. *Let $G = (\mathbb{Z}/q)^n$.*

(a) *$H^2(G)$ is generated by $H^2_{\mathrm{dec}}(G)$ and by the image of β_G.*
(b) *When $q = 2$ one has $H^2(G) = H^2_{\mathrm{dec}}(G)$.*

Proof. (a) follows from Proposition 2.9, Proposition 2.10, and the exact sequence (2.5). (b) follows from (a) and Lemma 2.4. □

3. Groups of Galois relation type

Let G be again a profinite group. The cup product $\cup\colon H^1(G) \times H^1(G) \to H^2(G)$ uniquely extends to a homomorphism

$$\cup\colon H^1(G) \otimes_{\mathbb{Z}} H^1(G) \to H^2(G), \quad \alpha \mapsto \cup\alpha. \tag{3.1}$$

Definition 3.1. We say that G has **Galois relation type** if:

(i) the kernel of the homomorphism (3.1) is generated by elements of the form $\psi \otimes \psi'$, where $\psi, \psi' \in H^1(G)$;
(ii) there exists $\xi \in H^1(G)$ such that for every $\psi \in H^1(G)$ one has $\psi \cup \xi + \beta_G(\psi) = 0$; and
(iii) the natural map $H^1(G) = H^1(G, \mathbb{Z}/q) \to H^1(G, \mathbb{Z}/p^i)$ is surjective for $1 \le i \le d$ (where $q = p^d$).

As a main example, consider a field F of characteristic $\neq p$ and containing a (fixed) primitive qth root of unity ζ_q. Let G_F be the absolute Galois group of F. Let $K_i^M(F)$ be the ith Milnor K-group of F, and consider the Galois symbol $K_i^M(F)/q \to H^i(G_F, \mathbb{Z}/q)$. It is an isomorphism for $i = 1, 2$, by the Kummer theory and the Merkurjev–Suslin theorem ([MeSu82], [GS06, Th. 8.6.5]), respectively. Moreover, it induces a commutative square

$$\begin{array}{ccc} (F^\times/(F^\times)^q) \otimes_{\mathbb{Z}} (F^\times/(F^\times)^q) & \xrightarrow{\sim} & H^1(G_F) \otimes_{\mathbb{Z}} H^1(G_F) \\ \downarrow & & \downarrow \cup \\ K_2^M(F)/q & \xrightarrow{\sim} & H^2(G_F). \end{array} \tag{3.2}$$

Here the left vertical map is given by

$$\sum_{i=1}^n (a_i(F^\times)^q \otimes b_i(F^\times)^q) \mapsto \sum_{i=1}^n \{a_i, b_i\} + qK_2^M(F)$$

and is surjective. Its kernel is the **Steinberg group**, generated by all $a(F^\times)^q \otimes b(F^\times)^q$ with $1 \in a(F^\times)^q + b(F^\times)^q$ [Efr06, §24.1]. We obtain:

Proposition 3.2. *$G = G_F$ has Galois relation type.*

Proof. By definition, the Steinberg group is generated by elements $a(F^\times)^q \otimes b(F^\times)^q$ which are mapped to 0 in $K_2^M(F)/q$. Now use the surjectivity (resp., injectivity) of the upper (resp., lower) horizontal map in (3.2) to deduce (i).

By Corollary 2.8(b), for $\psi \in H^1(G_F)$ one has $\beta_{G_F}(\psi) \cup \zeta_q = \psi \cup \kappa_q(\zeta_q)$, where on the left hand side we consider ζ_q as an element of $H^0(G_F, \mu_q)$. Identifying μ_q with $\mathbb{Z}/q$ via $\zeta_q^i \mapsto \bar{i}$, we get $\beta_{G_F}(\psi) = \psi \cup \kappa_q(\zeta_q)$ in $H^2(G_F, \mathbb{Z}/q) = H^2(G_F, \mu_q)$. Thus (ii) holds by taking $\xi = -\kappa_q(\zeta_q)$.

Finally, let $1 \le i \le d$. By Kummer's theory, the natural epimorphism $F^\times/(F^\times)^q \to F^\times/(F^\times)^{p^i}$ yields an epimorphism $H^1(G_F, \mathbb{Z}/q) \to H^1(G_F, \mathbb{Z}/p^i)$, proving (iii). □

Remark 3.3. Using also the surjectivity of the Galois symbol in dimension 2, one can strengthen Proposition 3.2 to Galois groups $G = \mathrm{Gal}(E/F)$, where E/F is a Galois extension, F contains a primitive

qth root of unity, and E has no proper p-extensions. Indeed, then $H^1(G_E) = 0$. In (3.2) all maps are surjective. Applying it for E, we obtain that $H^2(G_E) = 0$ as well. It therefore follows from the Hochschild–Serre spectral sequence that $\mathrm{inf}_{G_F}\colon H^i(G) \to H^i(G_F)$ is an isomorphism for $i = 1, 2$ [NSW00, Prop. 2.1.3]. Since the cup product and the Bockstein homomorphisms commute with inflation, conditions (i)–(iii) for G_F now transform into the analogous conditions for G.

4. Cohomology elements of simple type

For a profinite group G we define an abelian group $\Omega(G)$ by

$$\Omega(G) = \begin{cases} H^1(G) \otimes_{\mathbb{Z}} H^1(G), & \text{if } q = 2, \\ \big(H^1(G) \otimes_{\mathbb{Z}} H^1(G)\big) \oplus H^1(G), & \text{if } q \neq 2. \end{cases}$$

Define a homomorphism $\Lambda_G\colon \Omega(G) \to H^2(G)$ as follows:

$$\begin{aligned} \Lambda_G(\alpha) &= \cup\alpha, && \text{if } q = 2, \\ \Lambda_G(\alpha_1, \alpha_2) &= \cup\alpha_1 + \beta_G(\alpha_2), && \text{if } q \neq 2. \end{aligned}$$

The map $G \mapsto \Omega(G)$ is functorial. Given an epimorphism $G_1 \to G_2$ of profinite groups, the inflation map $\mathrm{inf}_{G_1}\colon H^1(G_2) \to H^1(G_1)$ induces a homomorphism $\mathrm{inf}_{G_1}\colon \Omega(G_2) \to \Omega(G_1)$ with a commutative square:

$$\begin{array}{ccc} \Omega(G_2) & \xrightarrow{\mathrm{inf}_{G_1}} & \Omega(G_1) \\ \downarrow{\scriptstyle \Lambda_{G_2}} & & \downarrow{\scriptstyle \Lambda_{G_1}} \\ H^2(G_2) & \xrightarrow{\mathrm{inf}_{G_1}} & H^2(G_1). \end{array} \tag{4.1}$$

Lemma 4.1. *Assume that G has Galois relation type and let $\tilde{G} = G/G^{(2)}$. Then $\Lambda_{\tilde{G}}$ is surjective.*

Proof. For $1 \leq i \leq d$, the natural map $H^1(G) \to H^1(G, \mathbb{Z}/p^i)$ is just the natural map $\mathrm{Hom}(\tilde{G}, \mathbb{Z}/q) \to \mathrm{Hom}(\tilde{G}, \mathbb{Z}/p^i)$, so by Definition 3.1(iii), it is surjective. Since additionally $\tilde{G}$ is abelian of exponent dividing q, it is therefore an inverse limit of finite groups $\tilde{G}_j$ of the form $(\mathbb{Z}/q)^{n_j}$. By Corollary 2.11, each $H^2(\tilde{G}_j)$ is generated by the images of $\cup$ and $\beta_{\tilde{G}_j}$ (and of $\cup$ only, if $q = 2$). Hence each $\Lambda_{\tilde{G}_j}$ is surjective. Conclude that $\Lambda_{\tilde{G}} = \varinjlim \Lambda_{\tilde{G}_j}$ is surjective. □

Definition 4.2. We say that $\alpha \in \Omega(G)$ has **simple type** if either:

(i) $q = 2$ and $\alpha = \psi \otimes \psi'$ for some $\psi, \psi' \in H^1(G)$; or
(ii) $q \neq 2$ and $\alpha = (\psi \otimes \psi', \psi)$ for some $\psi, \psi' \in H^1(G)$.

We call $M = \mathrm{Ker}(\psi) \cap \mathrm{Ker}(\psi')$ is a **kernel** of α (it may depend on ψ, ψ'). Observe that M is a normal open subgroup of G and that (ψ, ψ') induce an embedding of G/M in $(\mathbb{Z}/q)^2$. Hence $G^{(2)} \leq M$. Note that inflation homomorphisms map simple type elements to simple type elements.

Proposition 4.3. *Assume that G has Galois relation type. Then the group $\mathrm{Ker}(\Lambda_G)$ is generated by elements of simple type.*

Proof. For $q = 2$, this is just Definition 3.1(i).

So suppose that $q \neq 2$ and let $\alpha \in \mathrm{Ker}(\Lambda_G)$. There exists $\psi_0 \in H^1(G)$ with $\alpha - (0, \psi_0) \in (H^1(G) \otimes H^1(G)) \oplus \{0\}$. Take $\xi \in H^1(G)$ as in Definition 3.1(ii). Thus $\psi_0 \cup \xi + \beta_G(\psi_0) = 0$, i.e., $\Lambda_G(\psi_0 \otimes \xi, \psi_0) = 0$. Let $\alpha' = \alpha - (\psi_0 \otimes \xi, \psi_0)$. Then $\alpha' \in (H^1(G) \otimes H^1(G)) \oplus \{0\}$ and $\Lambda_G(\alpha') = \Lambda_G(\alpha) = 0$. By Definition 3.1(i), there exist $\psi_i, \psi'_i \in H^1(G)$, $i = 1, \dots, n$, with $\alpha' = \sum_{i=1}^n (\psi_i \otimes \psi'_i, 0)$ and $\psi_i \cup \psi'_i = 0$ for all i. For each i we have $\Lambda_G(\psi_i \otimes \xi, \psi_i) = 0$. Then

$$\alpha = (\psi_0 \otimes \xi, \psi_0) + \sum_{i=1}^n (\psi_i \otimes (\psi'_i + \xi), \psi_i) - \sum_{i=1}^n (\psi_i \otimes \xi, \psi_i). \tag{4.2}$$

Here all summands are simple type elements in $\mathrm{Ker}(\Lambda_G)$. □

Lemma 4.4. *Let $\alpha \in \mathrm{Ker}(\Lambda_G)$ have simple type and kernel M. Then there exist $\varphi \in H^1(M)^G$ and $\bar{\alpha} \in \Omega(G/M)$ of simple type and with trivial kernel, such that $\mathrm{inf}_G(\bar{\alpha}) = \alpha$ and $\Lambda_{G/M}(\bar{\alpha}) = \mathrm{trg}_{G/M}(\varphi)$.*

Proof. Take ψ, ψ' as in Definition 4.2 with $M = \mathrm{Ker}(\psi) \cap \mathrm{Ker}(\psi')$. There exist $\bar{\psi}, \bar{\psi}' \in H^1(G/M)$ such that $\mathrm{inf}_G(\bar{\psi}) = \psi$ and $\mathrm{inf}_G(\bar{\psi}') = \psi'$. We define $\bar{\alpha} \in \Omega(G/M)$ to be $\bar{\psi} \otimes \bar{\psi}'$, if $q = 2$, and $(\bar{\psi} \otimes \bar{\psi}', \bar{\psi})$, if $q \neq 2$. Thus $\bar{\alpha}$ has simple type and trivial kernel, and $\mathrm{inf}_G(\bar{\alpha}) = \alpha$. By (4.1) and (2.1), there is a commutative diagram with an exact row

$$\begin{array}{ccccc} & & \Omega(G/M) & \xrightarrow{\mathrm{inf}_G} & \Omega(G) \\ & & \downarrow{\scriptstyle \Lambda_{G/M}} & & \downarrow{\scriptstyle \Lambda_G} \\ H^1(M)^G & \xrightarrow{\mathrm{trg}_{G/M}} & H^2(G/M) & \xrightarrow{\mathrm{inf}_G} & H^2(G). \end{array}$$

It yields $\varphi \in H^1(M)^G$ as required. □

Definition 4.5. Call a subgroup N of G **distinguished** if there is an open subgroup M of G and elements $\varphi \in H^1(M)^G$ and $\bar{\alpha} \in \Omega(G/M)$, with $\bar{\alpha}$ of simple type and with trivial kernel, such that

$$\Lambda_{G/M}(\bar{\alpha}) = \mathrm{trg}_{G/M}(\varphi), \quad N = \mathrm{Ker}(\varphi).$$

In this case we say that $M, \varphi, \bar{\alpha}$ are **data** for N.

Remark 4.6. Since $\bar\alpha\in\Omega(G/M)$ has trivial kernel, G/M embeds in $(\mathbb{Z}/q)^2$. Hence $(G:N)=(G:M)(M:N)|q^3$ and $G^{(2)}\leq M$. Also, the exponent of G/N divides q^2.

Example 4.7. For every $\psi\in H^1(G)$, the subgroup $M=\mathrm{Ker}(\psi)$ of G is distinguished. Indeed, take $\bar\psi\in H^1(G/M)$ with $\mathrm{inf}_G(\bar\psi)=\psi$ and set $\bar\alpha=0\in\Omega(G/M)$. Trivially, $\bar\alpha=\bar\psi\otimes 0$ if $q=2$, and $\bar\alpha=(0\otimes\bar\psi,0)$ if $q\neq 2$. Thus $\bar\alpha$ has simple type and trivial kernel. For $\varphi=0\in H^1(M)^G$ we have $\mathrm{trg}_{G/M}(\varphi)=\Lambda_{G/M}(\bar\alpha)=0$ and $M=\mathrm{Ker}(\varphi)$.

5. $G^{(3)}$ AS AN INTERSECTION

Let G be again a profinite group, and let Δ_G be the intersection of all distinguished subgroups of G.

Proposition 5.1. $G^{(3)}\leq\Delta_G\leq G^{(2)}$.

Proof. Let N be a distinguished subgroup of G. Thus there exists an open normal subgroup M of G and $\varphi\in H^1(M)^G$ such that $\mathrm{Ker}(\varphi)=N$ and $G^{(2)}\leq M$. Hence Lemma 2.1 gives

$$G^{(3)}=(G^{(2)})^q[G^{(2)},G]\leq M^q[M,G]\leq\mathrm{Ker}(\varphi)=N.$$

Consequently, $G^{(3)}\leq\Delta_G$.

By Lemma 2.1 again, $\bigcap_{\psi\in H^1(G)}\mathrm{Ker}(\psi)=G^{(2)}$. Since each $\mathrm{Ker}(\psi)$ is distinguished (Example 4.7), we get that $\Delta_G\leq G^{(2)}$. □

Theorem 5.2. *If G has Galois relation type, then $G^{(3)}=\Delta_G$.*

Proof. By Proposition 5.1, $G^{(3)}\leq\Delta_G$.

For the converse inclusion, let $\tilde G=G/G^{(2)}$. It follows from Lemma 2.1 (with $N=G$) that the map $\mathrm{res}_{G^{(2)}}\colon H^1(G)\to H^1(G^{(2)})$ is trivial. Hence, by (2.1), $\mathrm{inf}_G\colon H^1(\tilde G)\to H^1(G)$ is an isomorphism. Consequently, $\mathrm{inf}_G\colon\Omega(\tilde G)\to\Omega(G)$ is also an isomorphism.

Now let $\varphi\in H^1(G^{(2)})^G$. By Lemma 4.1, $\Lambda_{\tilde G}$ is surjective, so there exists $\tilde\alpha\in\Omega(\tilde G)$ with $\mathrm{trg}_{\tilde G}(\varphi)=\Lambda_{\tilde G}(\tilde\alpha)$. By (4.1) and (2.1),

$$\Lambda_G(\mathrm{inf}_G(\tilde\alpha))=\mathrm{inf}_G(\Lambda_{\tilde G}(\tilde\alpha))=\mathrm{inf}_G(\mathrm{trg}_{\tilde G}(\varphi))=0.$$

By Proposition 4.3 we may therefore write $\mathrm{inf}_G(\tilde\alpha)=\sum_{i=1}^n\alpha_i$, where $\alpha_1,\dots,\alpha_n\in\mathrm{Ker}(\Lambda_G)$ have simple type.

For each $0 \le i \le n$ let M_i be a kernel for α_i. Recall that $G^{(2)} \le M_i$, so (4.1) again gives a commutative diagram

$$\begin{array}{ccccc} \Omega(G/M_i) & \xrightarrow{\inf_{\tilde G}} & \Omega(\tilde G) & \xrightarrow{\inf_G} & \Omega(G) \\ \downarrow{\scriptstyle \Lambda_{G/M_i}} & & \downarrow{\scriptstyle \Lambda_{\tilde G}} & & \downarrow{\scriptstyle \Lambda_G} \\ H^2(G/M_i) & \xrightarrow{\inf_{\tilde G}} & H^2(\tilde G) & \xrightarrow{\inf_G} & H^2(G). \end{array} \tag{5.1}$$

Lemma 4.4 gives rise to $\bar\alpha_i \in \Omega(G/M_i)$ of simple type and with trivial kernel and to $\varphi_i \in H^1(M_i)^G$ such that $\inf_G(\bar\alpha_i) = \alpha_i$ and $\Lambda_{G/M_i}(\bar\alpha_i) = \mathrm{trg}_{G/M_i}(\varphi_i)$. In particular, $\mathrm{Ker}(\varphi_i)$ is distinguished. For each i let $\tilde\alpha_i = \inf_{\tilde G}(\bar\alpha_i)$. It also has simple type, and one has $\alpha_i = \inf_G(\tilde\alpha_i)$. By (5.1), $\inf_G(\Lambda_{\tilde G}(\tilde\alpha_i)) = 0$. Moreover,

$$\inf_G(\tilde\alpha) = \textstyle\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \inf_G(\tilde\alpha_i).$$

But $\inf_G\colon \Omega(\tilde G) \to \Omega(G)$ is an isomorphism, so $\tilde\alpha = \sum_{i=1}^n \tilde\alpha_i$.

Next (2.1) and (2.2) give a commutative diagram with an exact row:

$$\begin{array}{ccccc} & & H^1(M_i)^G & \xrightarrow{\mathrm{trg}_{G/M_i}} & H^2(G/M_i) \\ & & \downarrow{\scriptstyle \mathrm{res}_{G^{(2)}}} & & \downarrow{\scriptstyle \inf_{\tilde G}} \\ 0 & \longrightarrow & H^1(G^{(2)})^G & \xrightarrow{\mathrm{trg}_{\tilde G}} & H^2(\tilde G). \end{array}$$

Using this and (5.1) we compute:

$$\begin{aligned} \mathrm{trg}_{\tilde G}(\varphi) = \Lambda_{\tilde G}(\tilde\alpha) &= \sum_{i=1}^n \Lambda_{\tilde G}(\tilde\alpha_i) = \sum_{i=1}^n \Lambda_{\tilde G}(\inf_{\tilde G}(\bar\alpha_i)) = \textstyle\sum_{i=1}^n \inf_{\tilde G}(\Lambda_{G/M_i}(\bar\alpha_i)) \\ &= \sum_{i=1}^n (\inf_{\tilde G} \circ \mathrm{trg}_{G/M_i})(\varphi_i) = \textstyle\sum_{i=1}^n (\mathrm{trg}_{\tilde G} \circ \mathrm{res}_{G^{(2)}})(\varphi_i). \end{aligned}$$

Since $\mathrm{trg}_{\tilde G}$ is injective, $\varphi = \sum_{i=1}^n \mathrm{res}_{G^{(2)}}(\varphi_i)$, so by Proposition 5.1,

$$\mathrm{Ker}(\varphi) \ge \bigcap_{i=1}^n \mathrm{Ker}(\mathrm{res}_{G^{(2)}}(\varphi_i)) = G^{(2)} \cap \bigcap_{i=1}^n \mathrm{Ker}(\varphi_i) \ge G^{(2)} \cap \Delta_G = \Delta_G.$$

Since $\varphi \in H^1(G^{(2)})^G$ was arbitrary, we deduce from Lemma 2.1 that

$$G^{(3)} = (G^{(2)})^q[G^{(2)}, G] = \bigcap_{\varphi \in H^1(G^{(2)})^G} \mathrm{Ker}(\varphi) \ge \Delta_G. \qquad \square$$

Corollary 5.3. *Let G be a profinite group of Galois relation type. Then $G^{(3)}$ is an intersection of normal open subgroups N of G with G/N of order dividing q^3 and exponent dividing q^2.*

6. Extensions

Let $\bar{G}$ be a finite group and A a finite trivial $\bar{G}$-module. We consider central extensions

$$\omega: \qquad 0 \to A \xrightarrow{f} B \xrightarrow{g} \bar{G} \to 1.$$

For a group isomorphism $\theta\colon \bar{G}' \to \bar{G}$ define an extension

$$\omega^\theta: \quad 0 \to A \xrightarrow{f} B \xrightarrow{\theta^{-1}\circ g} \bar{G}' \to 1.$$

When there is a commutative diagram of central extensions

$$\begin{array}{lccccccccc}
\omega: & 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & \bar{G} & \longrightarrow & 1 \\
 & & & \| & & \wr\downarrow h & & \| & & \\
\omega': & 0 & \longrightarrow & A' & \xrightarrow{f} & B' & \xrightarrow{g'} & \bar{G} & \longrightarrow & 1,
\end{array}$$

with h an isomorphism, ω and ω' are called **equivalent**. Let $\mathrm{Ext}(\bar{G}, A)$ be the set of all equivalence classes $[\omega]$ of extensions ω as above.

The **Baer sum** [CE56, Ch. XIV, §1] of central extensions

$$\omega_i: \qquad 0 \to A \xrightarrow{f_i} B_i \xrightarrow{g_i} \bar{G} \to 1, \quad i = 1, 2,$$

is the central extension

$$0 \to A \xrightarrow{\overline{(f_1,1)}=\overline{(1,f_2)}} B \xrightarrow{g_1=g_2} \bar{G} \to 1.$$

where for the fibred product $B_1 \times_{\bar{G}} B_2$ we set

$$B = (B_1 \times_{\bar{G}} B_2)/\{(f_1(a), f_2(a)^{-1}) \mid a \in A\}.$$

This induces an abelian group structure on $\mathrm{Ext}(\bar{G}, A)$, which is functorial in $\bar{G}$ (contravariantly) and in A (covariantly).

There is a canonical isomorphism $\mathrm{Ext}(\bar{G}, A) \cong H^2(\bar{G}, A)$ which is functorial in both $\bar{G}$ and A [NSW00, Th. 1.2.5]. Specifically, the cohomology class of an inhomogeneous normalized 2-cocycle $\alpha\colon \bar{G}^2 \to A$ corresponds to the class of $[\omega]$, where $B = A \times \bar{G}$ as sets, and the group law is given for $a, b \in A$ and $\sigma, \tau \in \bar{G}$ by

$$(a, \sigma) * (b, \tau) = (a + b + \alpha(\sigma, \tau), \sigma\tau). \tag{6.1}$$

Conversely, given ω as above, choose a set-theoretic section $s\colon \bar{G} \to B$ of g with $s(1) = 1$. The map $\alpha\colon \bar{G} \times \bar{G} \to A$, given by $\alpha(\bar{\sigma}_1, \bar{\sigma}_2) = s(\bar{\sigma}_1)s(\bar{\sigma}_2)s(\bar{\sigma}_1\bar{\sigma}_2)^{-1}$, is an inhomogenous normalized 2-cocyle whose cohomology class corresponds to $[\omega]$.

Remark 6.1 ([GS06, Remark 3.3.11], [Led05, p. 33])**.** Let $\bar{G} \to \tilde{G}$ be an epimorphism and let A be a $\tilde{G}$-module, whence a $\bar{G}$-module in the natural way. Then $\inf_{\bar G}\colon H^2(\tilde G, A) \to H^2(\bar G, A)$ corresponds to the map $\inf_{\bar G}\colon \operatorname{Ext}(\tilde G, A) \to \operatorname{Ext}(\bar G, A)$ sending the class of

$$\tilde\omega: \qquad 0 \to A \xrightarrow{f} B \xrightarrow{g} \tilde G \to 1$$

to the class of

$$\inf_{\bar G}(\tilde\omega): \quad 0 \to A \xrightarrow{(f,1)} B \times_{\tilde G} \bar G \xrightarrow{(b,\bar\sigma)\mapsto\bar\sigma} \bar G \to 1.$$

In particular we have:

Lemma 6.2. *Suppose that $\bar G = \tilde G \times \tilde G'$ and let $\tilde\omega$ be as above. Then $\inf_{\bar G}(\tilde\omega)$ is equivalent to*

$$0 \to A \xrightarrow{(f,1)} B \times \tilde G' \xrightarrow{g\times \mathrm{id}} \tilde G \times \tilde G' \to 1.$$

Proof. Use the commutative triangle

$$\begin{array}{ccc} B \times_{\tilde G} \bar G & \xrightarrow{(b,(\tilde\sigma,\tilde\sigma'))\mapsto(b,\tilde\sigma')} & B \times \tilde G' \\ & {\scriptstyle (b,(\tilde\sigma,\tilde\sigma'))\mapsto(\tilde\sigma,\tilde\sigma')} \searrow \quad \swarrow {\scriptstyle g\times\mathrm{id}} & \\ & \bar G & \end{array}$$

where the horizontal map is an isomorphism. □

7. Embedding problems

Let G be a profinite group. The following proposition is due to Hoechsmann [Hoe68, 2.1]:

Proposition 7.1. *Let M be an open normal subgroup of G. Consider the embedding problem*

(7.1)
$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & {\scriptstyle\Phi}\swarrow & \downarrow & & \\ \omega: & 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow G/M & \longrightarrow & 1 \end{array}$$

where A is a finite G/M-module, and let $\alpha \in H^2(G/M, A)$ be the cohomology class corresponding to $[\omega]$. Then the restriction map $\Phi \mapsto \varphi = \Phi|_M$ is a bijection between

(a) *the continuous homomorphisms $\Phi\colon G \to B$ making (7.1) commutative; and*
(b) *elements φ of $H^1(M, A)^G$ with $\operatorname{trg}_{G/M}(\varphi) = \alpha$.*

In particular, there exists Φ as in (a) if and only if $\inf_G(\alpha) = 0$.

Here the last sentence follows from the bijection using (2.1).

Now suppose that $A = \mathbb{Z}/q$ with the trivial G-action, where $q = p^d$.

Proposition 7.2. *Let M be an open normal subgroup of G and let $\bar\alpha\in\Omega(G/M)$ have simple type and trivial kernel. The following conditions on an open subgroup N of M are equivalent:*

(a) *N is a distinguished subgroup of G with data $M,\bar\alpha$;*
(b) *N is normal in G and there is a commutative diagram*

$$\begin{array}{ccccccccc} & & & & & & G/N & & \\ & & & & & \overset{h}{\swarrow} & \downarrow & & \\ \omega: & 0 & \longrightarrow & \mathbb{Z}/q & \longrightarrow & B & \longrightarrow G/M & \longrightarrow & 1, \end{array}$$

where ω is an extension corresponding to $\Lambda_{G/M}(\bar\alpha)$, the vertical map is the natural projection, and h is a monomorphism.

Proof. (a)⇒(b): By assumption, there exists $\varphi\in H^1(M)^G$ such that $\Lambda_{G/M}(\bar\alpha)=\mathrm{trg}_{G/M}(\varphi)\in H^2(G/M)$ and $N=\mathrm{Ker}(\varphi)$. In particular, N is normal in G. Choose a central extension ω as above corresponding to $\Lambda_{G/M}(\bar\alpha)$. Proposition 7.1 yields a continuous homomorphism $\Phi\colon G\to B$ such that (7.1) commutes and $\varphi=\Phi|_M$. Then $N=\mathrm{Ker}(\varphi)=M\cap\mathrm{Ker}(\Phi)$. Consequently, Φ induces a homomorphism $h\colon G/N\to B$ whose restriction to M/N is injective. It follows that h is also injective.

(b)⇒(a): Lift h to a homomorphism $\Phi\colon G\to B$ with kernel N. Then (7.1) commutes. Then $\varphi=\Phi|_M\in H^1(M)^G$. By Proposition 7.1, $\Lambda_{G/M}(\bar\alpha)=\mathrm{trg}_{G/M}(\varphi)$ and $N=M\cap\mathrm{Ker}(\Phi)=\mathrm{Ker}(\varphi)$, giving (a). □

8. Special extensions

Proposition 7.2 allows an explicit determination of the distinguished subgroups N of a profinite group G by means of the quotients G/N. We now carry this computation for $q=p$ prime, based on an analysis of several central extensions of small p-groups. We first recall the structure of the nonabelian groups of order p^3. When $p=2$ these are:

- the dihedral group of order 8,
$$D_4=\langle r,s\mid r^4=s^2=(rs)^2=1\rangle;$$
- the quaternionic group
$$Q_8=\langle r,s\mid r^4=1,\ [r,s]=r^2=s^2\rangle.$$

For p odd, there are two isomorphism types of groups of order p^3:

- the **Heisenberg group** of order p^3 and exponent p,
$$H_{p^3}=\langle r,s,t\mid r^p=s^p=t^p=1,\ [r,t]=[s,t]=1,\ [r,s]=t\rangle;$$

- the **extra-special group** of order p^3 and exponent p^2,

$$M_{p^3} = \langle r, s \mid r^{p^2} = s^p = 1,\ [r,s] = r^p \rangle.$$

8.1. **Remarks.** (a) When $p = 2$, $M_8 = D_4$. However, we will keep in this case the traditional notation D_4, and write M_{p^3} only when $p \neq 2$.

(b) Let G be one of the groups D_4, Q_8, when $p = 2$, or H_{p^3}, M_{p^3}, when $p \neq 2$. Then the unique normal subgroup of G of order p is its center, which coincides with the Frattini subgroup $G^{(2)}$ [MN77, §3.1]. Therefore $G^{(3)} = (G^{(2)})^p[G^{(2)}, G] = 1$.

(c) In M_{p^3} (for $p \neq 2$) one has $r^j s^i = s^i r^{(1+ip)j}$ for all $i, j \geq 0$. In particular, $[s, r^p] = 1$. Further, by induction, $(s^i r^j)^k = s^{ki} r^{(1+(k-1)ip/2)kj}$ for $k \geq 0$. It follows that $(s^i r^j)^p = 1$ if and only if $p | j$.

We define epimorphisms from these groups onto $(\mathbb{Z}/p)^2$ as follows:

$$\theta\colon D_4 \to (\mathbb{Z}/2)^2, \qquad r \mapsto (\bar 1, \bar 1),\ s \mapsto (\bar 0, \bar 1);$$
$$\lambda\colon H_{p^3} \to (\mathbb{Z}/p)^2, \qquad r \mapsto (\bar 1, \bar 0),\ s \mapsto (\bar 0, \bar 1),\ t \mapsto (\bar 0, \bar 0);$$
$$\lambda'\colon M_{p^3} \to (\mathbb{Z}/p)^2, \qquad r \mapsto (\bar 1, \bar 0),\ s \mapsto (\bar 0, \bar 1).$$

Remark 8.2. For later use we note that no proper subgroup of D_4 (resp., M_{p^3}) is mapped surjectively by θ (resp., λ').

The following central extensions will be needed in the sequel:

$$\omega_0: \quad 0 \to \mathbb{Z}/p \xrightarrow{\mathrm{id}} \mathbb{Z}/p \to 0 \to 0;$$
$$\omega_1: \quad 0 \to \mathbb{Z}/p \xrightarrow{\bar i \mapsto (\bar i, \bar 0)} (\mathbb{Z}/p)^2 \xrightarrow{(\bar i, \bar j) \mapsto \bar j} \mathbb{Z}/p \to 0;$$
$$\omega_2: \quad 0 \to \mathbb{Z}/p \xrightarrow{\bar i \mapsto \overline{pi}} \mathbb{Z}/p^2 \xrightarrow{\bar i \mapsto \bar i} \mathbb{Z}/p \to 0;$$
$$\omega_3: \quad 0 \to \mathbb{Z}/2 \xrightarrow{\bar i \mapsto r^{2i}} D_4 \xrightarrow{\theta} (\mathbb{Z}/2)^2 \to 0;$$
$$\omega_4: \quad 0 \to \mathbb{Z}/p \xrightarrow{\bar i \mapsto t^i} H_{p^3} \xrightarrow{\lambda} (\mathbb{Z}/p)^2 \to 0 \qquad (p \neq 2);$$
$$\omega_5: \quad 0 \to \mathbb{Z}/p \xrightarrow{\bar i \mapsto r^{pi}} M_{p^3} \xrightarrow{\lambda'} (\mathbb{Z}/p)^2 \to 0 \qquad (p \neq 2);$$
$$\omega_6: \quad 0 \to \mathbb{Z}/p \xrightarrow{\bar i \mapsto (\overline{pi}, 0)} (\mathbb{Z}/p^2) \oplus (\mathbb{Z}/p) \xrightarrow{(\bar i, \bar j) \mapsto (\bar i, \bar j)} (\mathbb{Z}/p)^2 \to 0.$$

Thus $[\omega_0]$, $[\omega_1]$ are the trivial classes of $\mathrm{Ext}(0, \mathbb{Z}/p)$, $\mathrm{Ext}(\mathbb{Z}/p, \mathbb{Z}/p)$, respectively, and $[\omega_1]$ is the inflation of $[\omega_0]$. Likewise

$$\mathrm{inf}_{(\mathbb{Z}/p)^2}([\omega_2]) = [\omega_6] \tag{8.1}$$

relative to the projection $\mathrm{pr}_1\colon (\mathbb{Z}/p)^2 \to \mathbb{Z}/p$ on the first coordinate.

Lemma 8.3. *For $p \neq 2$, the Baer sum of $[\omega_4]$ and $[\omega_6]$ is $[\omega_5]$.*

Proof. Let

$$\tilde B=\langle \tilde r,\tilde s,\tilde t\mid \tilde r^{p^2}=\tilde s^p=\tilde t^p=1,\ [\tilde r,\tilde t]=[\tilde s,\tilde t]=1,\ [\tilde r,\tilde s]=\tilde t\rangle.$$

There is a commutative square

$$\begin{array}{ccc} \tilde B & \xrightarrow{\quad j\quad} & H_{p^3} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \lambda} \\ (\mathbb{Z}/p^2)\oplus(\mathbb{Z}/p) & \xrightarrow{(\bar i,\bar j)\mapsto(\bar i,\bar j)} & (\mathbb{Z}/p)^2 \end{array},$$

where j maps $\tilde r,\tilde s,\tilde t$ to r,s,t, respectively, and f maps $\tilde r,\tilde s,\tilde t$ to $(\bar 1,\bar 0)$, $(\bar 0,\bar 1)$, $(\bar 0,\bar 0)$, respectively. Moreover, this square is cartesian, i.e.,

$$(j,f)\colon \tilde B\to H_{p^3}\times_{(\mathbb{Z}/p)^2}((\mathbb{Z}/p^2)\oplus(\mathbb{Z}/p))$$

is an isomorphism. The Baer sum is therefore the equivalence class of

$$0\ \to\ \mathbb{Z}/p\ \xrightarrow{\bar i\mapsto\tilde t^i}\ B=\tilde B/\langle(\tilde t^i\cdot\tilde r^{-pi})\mid \bar i\in\mathbb{Z}/p\rangle\ \xrightarrow{\lambda\circ j}\ (\mathbb{Z}/p)^2\ \to\ 0.$$

Hence B is obtained from $\tilde B$ by adding the relation $\tilde t=\tilde r^p$. Using Remark 8.1(c) we deduce that

$$B\cong\langle r,s\mid r^{p^2}=s^p=1,\ [s,r^p]=1,\ [r,s]=r^p\rangle=M_{p^3},$$

and the Baer sum is $[\omega_5]$. □

9. Extensions and simple type elements

We assume again that $q=p$ is prime. Let $\bar G$ be a finite group. In this section we compute the extensions corresponding to $\Lambda_{\bar G}(\bar\alpha)$ for $\bar\alpha\in\Omega(\bar G)$ of simple type and trivial kernel. Some of these facts are quite well-known in a Galois setting, as is systematically described in Ledet's book [Led05] (see also [Frö85, 7.7], [MN77]), but we derive them in a more abstract group-theoretic setting.

A) Cup products. Let $\bar\psi,\bar\psi'\in H^1(\bar G)$. We compute the extensions corresponding to $\bar\psi\cup\bar\psi'\in H^2(\bar G)$ in various situations. We use the notation $\omega^{\bar\psi}$ as in the beginning of §6. For the uniformity of the presentation we use this notation also when $\bar G\cong\mathbb{Z}/2$.

Proposition 9.1. *Suppose that* $\mathrm{Ker}(\bar\psi)\cap\mathrm{Ker}(\bar\psi')=1$.

(a) *If* $\bar\psi=\bar\psi'=0$*, then* $\bar\psi\cup\bar\psi'$ *corresponds to* ω_0.
(b) *If* $\bar\psi\neq0$, $\bar\psi'=0$ *(resp.,* $\bar\psi=0$, $\bar\psi'\neq0$*), then* $\bar\psi\cup\bar\psi'$ *corresponds to* $\omega_1^{\bar\psi}$ *(resp.,* $\omega_1^{\bar\psi'}$*).*
(c) *If* $p=2$ *and* $\bar\psi=\bar\psi'\neq0$*, then* $\bar\psi\cup\bar\psi'$ *corresponds to* $\omega_2^{\bar\psi}$.
(d) *If* $p\neq2$ *and* $\bar\psi,\bar\psi'\neq0$ *are* $\mathbb{F}_p$*-linearly dependent, then* $\bar\psi\cup\bar\psi'$ *corresponds to* $\omega_1^{\bar\psi}$.

(e) *If $p = 2$ and $\bar\psi, \bar\psi'$ are $\mathbb{F}_p$-linearly independent, then $\bar\psi \cup \bar\psi'$ corresponds to $\omega_3^{(\bar\psi,\bar\psi')}$.*
(f) *If $p \neq 2$ and $\bar\psi, \bar\psi'$ are $\mathbb{F}_p$-linearly independent, then $\bar\psi \cup \bar\psi'$ corresponds to $\omega_4^{(\bar\psi,\bar\psi')}$.*

Proof. Consider the central extension

$$\omega: \qquad 0 \to \mathbb{Z}/p \xrightarrow{f} B \xrightarrow{g} \bar G \to 1$$

corresponding to $\bar\psi \cup \bar\psi'$. An inhomogeneous normalized 2-cocyle $\bar G \times \bar G \to \mathbb{Z}/p$ representing $\bar\psi \cup \bar\psi'$ is given by $(\sigma,\tau) \mapsto \bar\psi(\sigma)\cdot\bar\psi'(\tau)$. Therefore $B = (\mathbb{Z}/p) \times \bar G$, with the group law

$$(a,\sigma) * (b,\tau) = (a + b + \bar\psi(\sigma)\bar\psi'(\tau), \sigma\tau) \tag{9.1}$$

for $a, b \in \mathbb{Z}/p$ and $\sigma, \tau \in \bar G$ (see (6.1)). The trivial element of B is $(0,1)$, and one has $f(a) = (a,1)$ and $g(a,\sigma) = \sigma$ for $a \in \mathbb{Z}/p$ and $\sigma \in \bar G$. By induction,

$$(a,\sigma)^i = (ia + \tfrac{i(i-1)}{2}\bar\psi(\sigma)\bar\psi'(\sigma), \sigma^i), \quad i = 0, 1, 2, \dots .$$

We examine the various possibilities.

(a) Immediate.

(b) Here $\bar\psi$ (resp., $\bar\psi'$) is an isomorphism $\bar G \to \mathbb{Z}/p$ and B is just the direct product $(\mathbb{Z}/p) \times \bar G$. The assertion follows.

(c) The assumptions imply that $\bar\psi = \bar\psi' \colon \bar G \to \mathbb{Z}/2$ is an isomorphism. Let σ_0 be the generator of $\bar G$. Then $(0,\sigma_0)^2 = (1,1)$ and $(0,\sigma_0)^4 = (0,1)$ in B. Hence $B \cong \mathbb{Z}/4$ and ω is equivalent to $\omega_2^{\bar\psi}$.

(d) Here $\bar\psi \colon \bar G \to \mathbb{Z}/p$ is an isomorphism. Since $p \neq 2$ and $\cup$ is alternate, $\bar\psi \cup \bar\psi' = 0$. Hence ω, and therefore also $\omega^{\bar\psi}$ split, so $B \cong (\mathbb{Z}/p)^2$. Moreover, pick $b \in B$ such that $(\bar\psi \circ g)(b) = \bar 1$. Then the map $B \to (\mathbb{Z}/p)^2$, $f(\bar 1) \mapsto (\bar 1, \bar 0)$, $b \mapsto (\bar 0, \bar 1)$, is an isomorphism making the following diagram commutative:

$$\begin{array}{lccccccccc}
\omega: & 0 & \longrightarrow & \mathbb{Z}/p & \xhookrightarrow{f} & B = (\mathbb{Z}/p) \times \bar G & \xrightarrow{g} & \bar G & \longrightarrow & 1 \\
 & & & \| & & \downarrow \wr & & \wr \downarrow \bar\psi & & \\
\omega_1: & 0 & \longrightarrow & \mathbb{Z}/p & \xhookrightarrow{\bar i \mapsto (\bar i, \bar 0)} & (\mathbb{Z}/p)^2 & \xrightarrow{(\bar i, \bar j) \mapsto \bar j} & \mathbb{Z}/p & \longrightarrow & 0.
\end{array}$$

Thus ω is equivalent to $\omega_1^{\bar\psi}$.

(e), (f) Here $(\bar\psi, \bar\psi') \colon \bar G \to (\mathbb{Z}/p)^2$ is an isomorphism. Take $\sigma_1, \sigma_2 \in \bar G$ with

$$\bar\psi(\sigma_1) = 1,\ \bar\psi(\sigma_2) = 0,\ \bar\psi'(\sigma_1) = 0,\ \bar\psi'(\sigma_2) = 1.$$

When $p=2$, we set $\tilde{r}=(1,\sigma_1\sigma_2)$, $\tilde{s}=(0,\sigma_2)$ and compute in B:

$$\tilde{r}^2=(1,1),\ \tilde{r}^4=(0,1),\ \tilde{s}^2=(0,1),\ \tilde{r}\tilde{s}=(0,\sigma_1),\ (\tilde{r}\tilde{s})^2=(0,1).$$

We get an isomorphism $B\cong D_4$, $\tilde{r}\mapsto r$, $\tilde{s}\mapsto s$, and a diagram

$$\begin{array}{lccccccccc}
\omega: & 0 & \longrightarrow & \mathbb{Z}/2 & \overset{f}{\hookrightarrow} & B=(\mathbb{Z}/2)\times\bar{G} & \overset{g}{\longrightarrow} & \bar{G} & \longrightarrow & 1\\
 & & & \| & & \downarrow\wr & & \downarrow\wr\,(\bar\psi,\bar\psi') & & \\
\omega_3: & 1 & \longrightarrow & \mathbb{Z}/2 & \xrightarrow{\bar{i}\mapsto r^{2i}} & D_4 & \overset{\theta}{\longrightarrow} & (\mathbb{Z}/2)^2 & \longrightarrow & 0
\end{array}$$

which is commutative with exact rows. Hence ω is equivalent to $\omega_3^{(\bar\psi,\bar\psi')}$.

For p odd, B has exponent p. Set $\tilde{r}=(0,\sigma_1)$, $\tilde{s}=(0,\sigma_2)$, $\tilde{t}=(1,1)$. Then

$$\tilde{r}\tilde{t}=\tilde{t}\tilde{r}=(1,\sigma_1),\quad \tilde{s}\tilde{t}=\tilde{t}\tilde{s}=(1,\sigma_2),\quad \tilde{r}\tilde{s}=\tilde{t}\tilde{s}\tilde{r}=(1,\sigma_1\sigma_2).$$

This gives an isomorphism $B\cong H_{p^3}$, $\tilde{r}\mapsto r$, $\tilde{s}\mapsto s$, $\tilde{t}\mapsto t$, and a commutative diagram

$$\begin{array}{lccccccccc}
\omega: & 0 & \longrightarrow & \mathbb{Z}/p & \overset{f}{\hookrightarrow} & B=(\mathbb{Z}/p)\times\bar{G} & \overset{g}{\longrightarrow} & \bar{G} & \longrightarrow & 1\\
 & & & \| & & \downarrow\wr & & \downarrow\wr\,(\bar\psi,\bar\psi') & & \\
\omega_4: & 0 & \longrightarrow & \mathbb{Z}/p & \xrightarrow{\bar{i}\mapsto t^{i}} & H_{p^3} & \overset{\lambda}{\longrightarrow} & (\mathbb{Z}/p)^2 & \longrightarrow & 0.
\end{array}$$

Therefore ω is equivalent in this case to $\omega_4^{(\bar\psi,\bar\psi')}$. □

B) Bockstein elements.

Proposition 9.2. *If $0\neq\bar\psi\in H^1(\bar{G})$ and $\bar{G}\cong\mathbb{Z}/p$, then $\beta_{\bar{G}}(\bar\psi)$ corresponds to $\omega_2^{\bar\psi}$.*

Proof. As a connecting homomorphism in a cohomology exact sequence, $\beta_{\bar{G}}\colon H^1(\bar{G})\to H^2(\bar{G})$ is defined as follows [NSW00, Ch. I, §3]: let $\mathrm{pr}\colon\mathbb{Z}/p^2\to\mathbb{Z}/p$ be the natural projection. Given a nonzero $\bar\psi\in H^1(\bar{G})$, we consider it as an inhomogeneous 1-cocycle, and lift it to a map $\hat\psi\colon\bar{G}\to\mathbb{Z}/p^2$ with $\bar\psi=\mathrm{pr}\circ\hat\psi$. Then the map

$$\chi\colon\bar{G}\times\bar{G}\to\mathbb{Z}/p,\qquad \chi(\sigma_1,\sigma_2)=\hat\psi(\sigma_1)+\hat\psi(\sigma_2)-\hat\psi(\sigma_1\sigma_2)$$

is a normalized 2-cocycle with cohomology class $\beta_{\bar{G}}(\bar\psi)$.

On the other hand, $\bar\psi\colon\bar{G}\to\mathbb{Z}/p$ is an isomorphism, so $\hat\psi$ is a section of the epimorphism $\bar\psi^{-1}\circ\mathrm{pr}\colon\mathbb{Z}/p^2\to\bar{G}$. By the remarks in §6, the cohomology class $\beta_{\bar{G}}(\bar\psi)$ of χ therefore corresponds to the extension

$$\omega_2^{\bar\psi}:\qquad 0\ \to\ \mathbb{Z}/p\ \to\ \mathbb{Z}/p^2\ \xrightarrow{\bar\psi^{-1}\circ\mathrm{pr}}\ \bar{G}\ \to\ 1.$$ □

Corollary 9.3. *Suppose that $p \neq 2$ and let $\bar\psi, \bar\psi' \in H^1(\bar G)$ be $\mathbb{F}_p$-linearly dependent, $\bar\psi \neq 0$. Then $\Lambda_{\bar G}(\bar\psi \otimes \bar\psi', \bar\psi)$ corresponds to $\omega_2^{\bar\psi}$.*

Proof. Since $\cup$ is alternate, $\bar\psi \cup \bar\psi' = 0$. Hence $\Lambda_{\bar G}(\bar\psi \otimes \bar\psi', \bar\psi) = \beta_{\bar G}(\bar\psi)$. Now use Proposition 9.2. □

When $\bar\psi, \bar\psi'$ are $\mathbb{F}_p$-linearly independent the computation is more involved. It is sufficient for us to consider only the case $p \neq 2$.

Proposition 9.4. *Suppose that $p \neq 2$. Let $\bar\psi, \bar\psi' \in H^1(\bar G)$ be $\mathbb{F}_p$-linearly independent with* $\mathrm{Ker}(\bar\psi) \cap \mathrm{Ker}(\bar\psi') = 1$. *Then $\Lambda_{\bar G}(\bar\psi \otimes \bar\psi', \bar\psi)$ corresponds to $\omega_5^{(\bar\psi,\bar\psi')}$.*

Proof. We may decompose $\bar G = \tilde G \times \tilde G'$, where $\tilde G, \tilde G' \cong \mathbb{Z}/p$ and there exists $\tilde\psi \in H^1(\tilde G)$ with $\inf_{\bar G}(\tilde\psi) = \bar\psi$. By Proposition 9.2, $\beta_{\tilde G}(\tilde\psi)$ corresponds to $\omega_2^{\tilde\psi}$. Hence $\beta_{\bar G}(\bar\psi) = \inf_{\bar G}(\beta_{\tilde G}(\tilde\psi))$ corresponds to $\inf_{\bar G}(\omega_2^{\tilde\psi})$. By Lemma 6.2, this extension is

$$0 \to \mathbb{Z}/p \xrightarrow{\bar i \mapsto (\overline{pi},1)} (\mathbb{Z}/p^2) \times \tilde G' \xrightarrow{(\tilde\psi^{-1}\circ \mathrm{pr},\mathrm{id})} \tilde G \times \tilde G' \to 1,$$

where $\mathrm{pr}\colon \mathbb{Z}/p^2 \to \mathbb{Z}/p$ is again the natural projection. But the latter extension is equivalent to

$$0 \to \mathbb{Z}/p \xrightarrow{\bar i \mapsto (\overline{pi},0)} (\mathbb{Z}/p^2) \times (\mathbb{Z}/p) \xrightarrow{(\bar\psi^{-1}\circ \mathrm{pr},(\bar\psi')^{-1})} \bar G = \tilde G \times \tilde G' \to 1,$$

which is $\omega_6^{(\bar\psi,\bar\psi')}$.

Now by Proposition 9.1(f), $\bar\psi \cup \bar\psi'$ corresponds to $\omega_4^{(\bar\psi,\bar\psi')}$. It therefore follows from Lemma 8.3 that $\bar\psi \cup \bar\psi' + \beta_{\bar G}(\bar\psi)$ corresponds to $\omega_5^{(\bar\psi,\bar\psi')}$. □

C) Summary. Putting together the results of the previous two subsections we obtain:

Proposition 9.5. *Let $\bar\alpha \in \Omega(\bar G)$ have simple type and trivial kernel. Then $\Lambda_{\bar G}(\bar\alpha) \in H^2(\bar G)$ corresponds to one of the following extensions:*

(i) *when $p = 2$:* ω_0, $\omega_1^{\bar\psi}$, $\omega_2^{\bar\psi}$, $\omega_3^{(\bar\psi,\bar\psi')}$;

(ii) *when $p \neq 2$:* ω_0, $\omega_1^{\bar\psi}$, $\omega_2^{\bar\psi}$, $\omega_5^{(\bar\psi,\bar\psi')}$,

where $\bar\psi, \bar\psi'$ are taken as above.

Proof. When $p = 2$ we have $\bar\alpha = \bar\psi \otimes \bar\psi'$, with $\bar\psi, \bar\psi' \in H^1(\bar G)$ and $\mathrm{Ker}(\bar\psi) \cap \mathrm{Ker}(\bar\psi') = 1$. Furthermore, $\Lambda_{\bar G}(\bar\alpha) = \bar\psi \cup \bar\psi'$. Now apply Proposition 9.1.

When $p \neq 2$ we write $\bar\alpha = (\bar\psi \otimes \bar\psi', \bar\psi)$ where again $\bar\psi, \bar\psi' \in H^1(\bar G)$ and $\mathrm{Ker}(\bar\psi) \cap \mathrm{Ker}(\bar\psi') = 1$. Here $\Lambda_{\bar G}(\bar\alpha) = \bar\psi \cup \bar\psi' + \beta_{\bar G}(\bar\psi)$. If $\bar\psi = 0$, then this corresponds to either ω_0 or $\omega_1^{\bar\psi}$, by Proposition 9.1(a)(b). If $\bar\psi \neq 0$ and $\bar\psi, \bar\psi'$ are $\mathbb{F}_p$-linearly dependent, then $\Lambda_{\bar G}(\bar\alpha) = \beta_{\bar G}(\bar\psi)$ corresponds to $\omega_2^{\bar\psi}$, by Proposition 9.2. Finally, if $\bar\psi,\bar\psi'$ are $\mathbb{F}_p$-linearly independent, then by Proposition 9.4, $\Lambda_{\bar G}(\bar\alpha)$ corresponds to $\omega_5^{(\bar\psi,\bar\psi')}$. □

One has the following converse result:

Proposition 9.6. *When $p=2$ let $i\in\{0,1,2,3\}$ and when $p\neq 2$ let $i\in\{0,1,2,5\}$. Let $(\mathbb{Z}/p)^s$ be the right group in ω_i (so $s=0,1,1,2,2$ for $i=0,1,2,3,5$, respectively). Let $\theta\colon \bar G\xrightarrow{\sim}(\mathbb{Z}/p)^s$ be an isomorphism. There exists $\bar\alpha\in\Omega(\bar G)$ of simple type and with trivial kernel such that $\Lambda_{\bar G}(\bar\alpha)\in H^2(\bar G)$ corresponds to ω_i^θ.*

Proof. We may assume that $\bar G=(\mathbb{Z}/p)^s$ and $\theta=\mathrm{id}$. Let $\mathrm{pr}_j\colon(\mathbb{Z}/p)^2\to\mathbb{Z}/p$ be the projection on the jth coordinate, $j=1,2$.

When $p=2$ we take $\bar\alpha=\bar\psi\otimes\bar\psi'$, where

$$(\bar\psi,\bar\psi')=(0,0),\ (\mathrm{id}_{\mathbb{Z}/2},0),\ (\mathrm{id}_{\mathbb{Z}/2},\mathrm{id}_{\mathbb{Z}/2}),\ (\mathrm{pr}_1,\mathrm{pr}_2),$$

to obtain using Proposition 9.1(a)(b)(c)(e) ω_0, ω_1, ω_2, ω_3, respectively.

When $p\neq 2$ we take $\bar\alpha=(\bar\psi\otimes\bar\psi',\bar\psi)$, where $(\bar\psi,\bar\psi')=(0,0),\ (0,\mathrm{id}_{\mathbb{Z}/p})$, to obtain using Proposition 9.1(a)(b) the extensions ω_0, ω_1, respectively. Also, take $\bar\alpha=(\bar\psi\otimes\bar\psi',\bar\psi)$, where $\bar\psi=\bar\psi'=\mathrm{id}_{\mathbb{Z}/p}$ to obtain using Corollary 9.3 the extension ω_2. Finally, $\bar\alpha=(\bar\psi\otimes\bar\psi',\bar\psi)$, where $\bar\psi=\mathrm{pr}_1$, $\bar\psi'=\mathrm{pr}_2$, gives using Proposition 9.4 the extension ω_5. □

10. Lifting of homomorphisms

We now apply the computations of the previous section to solve some specific embedding problems.

Lemma 10.1. *Let G be a profinite group and $\psi\colon G\to\mathbb{Z}/p$ an epimorphism. Then $\beta_G(\psi)=0$ if and only if ψ factors via the natural map $\mathbb{Z}/p^2\to\mathbb{Z}/p$.*

Proof. Let $\bar G=G/\mathrm{Ker}(\psi)\cong\mathbb{Z}/p$ and let $\pi\colon G\to\bar G$ be the natural map. There exists $\bar\psi\in H^1(\bar G)$ with $\psi=\bar\psi\circ\pi$ and $\mathrm{inf}_G(\bar\psi)=\psi$. Then $\mathrm{inf}_G(\beta_{\bar G}(\bar\psi))=\beta_G(\psi)$. By Proposition 9.2, $\beta_{\bar G}(\bar\psi)$ corresponds to $\omega_2^{\bar\psi}$. It follows from the last sentence of Proposition 7.1 that $\beta_G(\psi)=0$ if and only if the following embedding problem is solvable

$$\begin{array}{ccccc} & & G & & \\ & \overset{\Phi}{\swarrow} & \downarrow{\scriptstyle\psi} & & \\ \mathbb{Z}/p^2 & \longrightarrow & \mathbb{Z}/p & \longrightarrow & 0. \end{array}$$

Note that if the homomorphism Φ exists, then it must be surjective. □

In the next proposition let r,s be the generators of M_{p^3} as in §8.

Proposition 10.2. *Let $p \neq 2$ and let G be a profinite group of Galois relation type. Every epimorphism $\psi\colon G \to \mathbb{Z}/p$ breaks via one of the epimorphisms:*

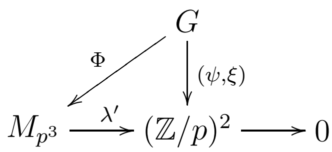
(i) *the natural map $\mathbb{Z}/p^2 \to \mathbb{Z}/p$;*
(ii) *the map $\lambda'' \colon M_{p^3} \to \mathbb{Z}/p$, defined by $r \mapsto \bar{1}$, $s \mapsto \bar{0}$.*

Proof. If $\beta_G(\psi) = 0$, then by Lemma 10.1, ψ breaks via the map (i).

Next assume that $\beta_G(\psi) \neq 0$. Since G has Galois relation type, there exists $\xi \in H^1(G)$ with $\psi \cup \xi + \beta_G(\psi) = 0$. In particular, $\psi \cup \xi \neq 0$. Since $p \neq 2$ and the cup product is alternate, ψ and ξ are $\mathbb{F}_p$-linearly independent. Now let $\bar{G} = G/(\mathrm{Ker}(\psi) \cap \mathrm{Ker}(\xi)) \cong (\mathbb{Z}/p)^2$, and let $\pi\colon G \to \bar{G}$ be the canonical map. Take $\bar{\psi}, \bar{\xi} \in H^1(\bar{G})$ with $\psi = \bar{\psi} \circ \pi$, $\xi = \bar{\xi} \circ \pi$, $\mathrm{inf}_G(\bar{\psi}) = \psi$, and $\mathrm{inf}_G(\bar{\xi}) = \xi$. Then

$$\mathrm{inf}_G(\Lambda_{\bar{G}}(\bar{\psi} \otimes \bar{\xi}, \bar{\psi})) = \Lambda_G(\psi \otimes \xi, \psi) = 0.$$

By Proposition 9.4, $\Lambda_{\bar{G}}(\bar{\psi} \otimes \bar{\xi}, \bar{\psi})$ corresponds to $\omega_5^{(\bar{\psi},\bar{\xi})}$. It follows again from Proposition 7.1 that the embedding problem



is solvable. By Remark 8.2, no proper subgroup of M_{p^3} is mapped surjectively by λ'. Therefore Φ is surjective. As before, let $\mathrm{pr}_1\colon (\mathbb{Z}/p)^2 \to \mathbb{Z}/p$ be the projection on the first coordinate. We deduce that ψ breaks via the epimorphism $\mathrm{pr}_1 \circ \lambda'$, which is just λ''. □

Next let r, s be the generators of D_4 as in §8. We write $G(p)$ for the maximal pro-p quotient of the profinite group G. One has the following analog of Proposition 10.2 for $p = 2$.

Proposition 10.3. *Let $p = 2$ and let G be a profinite group of Galois relation type and such that $G(2) \ncong \mathbb{Z}/2$. Every epimorphism $\psi\colon G \to \mathbb{Z}/2$ factors via one of the epimorphisms:*

(i) *the natural map $\mathbb{Z}/4 \to \mathbb{Z}/2$;*
(ii) *the map $\theta'\colon D_4 \to \mathbb{Z}/2$, defined by $r \mapsto \bar{1}$, $s \mapsto \bar{0}$;*
(iii) *the map $\theta'' \colon D_4 \to \mathbb{Z}/2$, defined by $r \mapsto \bar{0}$, $s \mapsto \bar{1}$.*

Proof. Let ξ be as in Definition 3.1(ii). By the assumptions, $G(2) \neq 1, \mathbb{Z}/2$. Hence, if $G(2)$ is pro-cyclic, then ψ factors via the map (i). We may therefore assume that $G(2)$ is not pro-cyclic.

If $\beta_G(\psi) = 0$, then by Lemma 10.1, ψ factors via the map (i).

Next we assume that $\psi, \xi + \psi$ are $\mathbb{F}_2$-linearly independent. Let $\bar{G} = G/(\ker(\psi) \cap \mathrm{Ker}(\xi))$ and let $\pi\colon G \to G/\bar{G}$ be the natural map. There exist $\bar\psi,\bar\xi \in H^1(\bar G)$ with $\psi = \bar\psi\circ\pi$, $\xi = \bar\xi\circ\pi$, $\inf_G(\bar\psi) = \psi$ and $\inf_G(\bar\xi) = \xi$. Note that $\mathrm{Ker}(\bar\psi)\cap\mathrm{Ker}(\bar\xi+\bar\psi) = \mathrm{Ker}(\bar\psi)\cap\ker(\bar\xi) = 1$. By Proposition 9.1(e), $\bar\psi\cup(\bar\xi+\bar\psi)$ corresponds to the extension $\omega_3^{(\bar\psi,\bar\xi+\bar\psi)}$. By the choice of ξ and Lemma 2.4,

$$\inf_G(\bar\psi\cup(\bar\xi+\bar\psi)) = \psi\cup\xi+\psi\cup\psi = 2\beta_G(\psi) = 0.$$

Proposition 7.1 therefore implies that the embedding problem

$$\begin{array}{ccccc} & & G & & \\ & \swarrow^{\Phi} & \downarrow{\scriptstyle(\psi,\xi+\psi)} & & \\ D_4 & \xrightarrow{\theta} & (\mathbb{Z}/2)^2 & \longrightarrow & 0 \end{array}$$

is solvable. Since no proper subgroup of D_4 is mapped by θ surjectively onto $(\mathbb{Z}/2)^2$ (Remark 8.2), Φ is surjective. We deduce that ψ factors via the epimorphism $\mathrm{pr}_1\circ\theta$, which is just θ'.

Finally assume that $\beta_G(\psi)\neq 0$ and $\psi,\xi+\psi$ are $\mathbb{F}_2$-linearly dependent. As $\beta_G(\psi) = \psi\cup\xi$, necessarily $\xi\neq 0$. But $\psi\neq 0$, so $\psi = \xi$.

Now $G(2)$ is not pro-cyclic, so there exists $\psi'\in H^1(G)$ such that ψ,ψ' are $\mathbb{F}_2$-linearly independent. Then $\psi',\xi+\psi'$ are also $\mathbb{F}_2$-linearly independent. By the argument above, the embedding problem

$$\begin{array}{ccccc} & & G & & \\ & \swarrow^{\Phi} & \downarrow{\scriptstyle(\psi',\xi+\psi')} & & \\ D_4 & \xrightarrow{\theta} & (\mathbb{Z}/2)^2 & \longrightarrow & 0 \end{array}$$

is solvable. Composing with the map $\sigma\colon(\mathbb{Z}/2)^2\to\mathbb{Z}/2$, $(\bar i,\bar j)\mapsto\overline{i+j}$, we obtain that $\psi=\xi$ factors via $\sigma\circ\theta$, which is just θ''. □

11. The main results

Let G be a again a profinite group and $q = p$ a prime number.

Theorem 11.1. *The following conditions on a normal open subgroup N of G are equivalent:*

(a) *N is distinguished;*

(b) (i) *When $p = 2$, G/N is isomorphic to one of the groups*

$$1,\ \mathbb{Z}/2,\ (\mathbb{Z}/2)^2,\ \mathbb{Z}/4,\ D_4;$$

(ii) *When $p\neq 2$, G/N is isomorphic to one of the groups*

$$1,\ \mathbb{Z}/p,\ (\mathbb{Z}/p)^2,\ \mathbb{Z}/p^2,\ M_{p^3}.$$

Proof. (a)⇒(b): Let N be distinguished and M, $\bar{\alpha}$, φ data for N. Thus $N = \mathrm{Ker}(\varphi)$. Set $\bar{G} = G/M$ and consider a central extension

$$\omega : \qquad 0 \to \mathbb{Z}/p \to B \to \bar{G} \to 1$$

corresponding to $\Lambda_{\bar{G}}(\bar{\alpha})$. By Proposition 7.2, G/N embeds in B.

If $p = 2$, then by Proposition 9.5, ω is equivalent to an extension of one of the forms ω_0, $\omega_1^{\bar{\psi}}$, $\omega_2^{\bar{\psi}}$, $\omega_3^{(\bar{\psi},\bar{\psi}')}$. Then G/N embeds in one of the groups $\mathbb{Z}/2$, $(\mathbb{Z}/2)^2$, $\mathbb{Z}/4$, D_4, and is therefore as in (i).

If $p \neq 2$, then by Proposition 9.5, ω is equivalent to an extension of one of the forms ω_0, $\omega_1^{\bar{\psi}}$, $\omega_2^{\bar{\psi}}$, $\omega_5^{(\bar{\psi},\bar{\psi}')}$. Then G/N embeds in one of the groups $\mathbb{Z}/p$, $(\mathbb{Z}/p)^2$, $\mathbb{Z}/p^2$, M_{p^3}, and is therefore as in (ii).

(b)⇒(a): By Example 4.7, G itself is distinguished. We may therefore assume that G/N is nontrivial. Hence it is isomorphic to the middle group B of ω_i where $i \in \{0,1,2,3\}$, if $p = 2$, and $i \in \{0,1,2,5\}$, if $p \neq 2$. Therefore there is an open normal subgroup M of G such that $N \leq M$ and the following diagram commutes:

$$\begin{array}{lccccccccc}
\omega : & 0 & \longrightarrow & \mathbb{Z}/p & \longrightarrow & G/N & \longrightarrow & G/M & \longrightarrow & 1 \\
 & & & \| & & \wr\downarrow & & \wr\downarrow\theta & & \\
\omega_i : & 0 & \longrightarrow & \mathbb{Z}/p & \longrightarrow & B & \longrightarrow & (\mathbb{Z}/p)^s & \longrightarrow & 0,
\end{array}$$

where θ is an isomorphism. Then ω, ω_i^θ are equivalent. By Proposition 9.6, ω_i^θ corresponds to $\Lambda_{G/M}(\bar{\alpha}) \in H^2(G/M)$ for some $\bar{\alpha} \in \Omega(G/M)$ of simple type and with trivial kernel, and therefore so does ω. Conclude from Proposition 7.2 that N is distinguished. □

We deduce the following stronger form of the Main Theorem:

Corollary 11.2. *Suppose that* $p \neq 2$ *and let* G *be a profinite group of Galois relation type. Then* $G^{(3)}$ *is the intersection of all normal open subgroups* N *of* G *with* G/N *isomorphic to one of* 1, $\mathbb{Z}/p^2$, M_{p^3}.

Proof. By Theorems 5.2 and 11.1, $G^{(3)}$ is the intersection of all normal open subgroups N of G with G/N isomorphic to one of 1, $\mathbb{Z}/p$, $\mathbb{Z}/p^2$, M_{p^3}. By Proposition 10.2, $\mathbb{Z}/p$ can be omitted from this list. □

For $p = 2$ Theorem 5.2 and Theorem 11.1 give:

Corollary 11.3. *Let* $p = 2$ *and let* G *be of Galois relation type. Then* $G^{(3)}$ *is the intersection of all normal open subgroups* N *of* G *such that* G/N *is isomorphic to one of the groups* 1, $\mathbb{Z}/2$, $\mathbb{Z}/4$, D_4.

By Proposition 3.2, this extends [MSp96, Cor. 2.18], which proves it for $G = G_F$, F a field. Combined with Proposition 10.3 it gives:

Corollary 11.4. *Let $p = 2$ and let G be a profinite group of Galois relation type such that $G(2) \not\cong \mathbb{Z}/2$. Then $G^{(3)}$ is the intersection of all normal open subgroups N of G such that G/N is isomorphic to one of the groups 1, $\mathbb{Z}/4$, D_4.*

11.5. **Remarks.** (a) The converse of Corollary 11.4 also holds: if $G(2) \cong \mathbb{Z}/2$, then $G^{(3)}$ is not an intersection as above.

(b) Let F be a field of characteristic $\neq 2$ and let $G = G_F$. Then $G(2) \cong \mathbb{Z}/2$ if and only if F is a Euclidean field, i.e., the set $(F^\times)^2$ of all nonzero squares in F is an ordering on F ([Bec74], [Efr06, §19.2]). Therefore, by (a), the Euclidean fields are those fields for which the group $\mathbb{Z}/2$ cannot be omitted from the list in Corollary 11.3.

12. The structure of $G/G^{(3)}$

When $p = 2$ and $G = G_F$ for a field F, the quotient $G/G^{(3)}$ is the W**-group** of F, studied in [MSp90], [MSp96], and [MMS04]. It encodes much of the "real" arithmetic structure of F. We now give some restrictions on the group structure of $G/G^{(3)}$ also for p odd.

Proposition 12.1. *Let G be a profinite group of Galois relation type with $G/G^{(3)}$ nonabelian.*

(a) *If $p \neq 2$, then M_{p^3} is a quotient of $G/G^{(3)}$.*
(b) *If $p = 2$, then D_8 is a quotient of $G/G^{(3)}$.*

Proof. By our assumption, $G^{(3)}$ cannot be an intersection of open normal subgroups N of G with G/N abelian. When $p \neq 2$ (resp., $p = 2$) Corollary 11.2 (resp., Corollary 11.3) yields an open normal subgroup N of G with $G/N \cong M_{p^3}$ (resp., $G/N \cong D_4$). The natural epimorphism $h\colon G \to \bar{G} = G/N$ maps $G^{(3)}$ to $\bar{G}^{(3)}$, which is trivial by Remark 8.1(b). Hence h induces an epimorphism $\bar{h}\colon G/G^{(3)} \to \bar{G}$. □

We recover the following known "automatic realizations":

Corollary 12.2. *Suppose that F is a field of characteristic $\neq p$ and containing a root of unity of order p.*

(a) ([Bra89]) *If $p \neq 2$ and H_{p^3} is realizable as a Galois group over F, then M_{p^3} is also realizable as a Galois group over F.*
(b) ([MS91, Prop. 2.1]) *If $p = 2$ and Q_8 is realizable as a Galois group over F, then D_4 is also realizable over F.*

Proof. When $p \neq 2$ (resp., $p = 2$), take $\bar{G} = H_{p^3}$ (resp., $\bar{G} = Q_8$). Thus $\bar{G}$ is a quotient of $G = G_F$, and as $\bar{G}^{(3)} = 1$ (by Remark 8.1(b)), also of $G/G^{(3)}$. Hence $G/G^{(3)}$ is nonabelian. Now apply Proposition 12.1. □

The next fact was earlier proved in [BLMS07, Th. A.3] when $G = G_F$ for a field F containing a primitive pth root of unity.

Proposition 12.3. *Let $p \neq 2$ and let G be a profinite group of Galois relation type. Every element of $G/G^{(3)}$ of order p belongs to $G^{(2)}/G^{(3)}$.*

Proof. It suffices to show that the elements of order p in $G/G^{(3)}$ are in the kernel of every epimorphism $\bar{\psi}\colon G/G^{(3)} \to \mathbb{Z}/p$. Now $\bar{\psi}$ lifts to a unique epimorphism $\psi\colon G \to \mathbb{Z}/p$. By Proposition 10.2, ψ breaks via an epimorphism $\pi\colon \bar{G} \to \mathbb{Z}/p$, where either $\bar{G} = \mathbb{Z}/p^2$ and π is the natural projection, or $\bar{G} = M_{p^3}$ and $\pi = \lambda''$ (where λ'' maps the generators r, s of M_{p^3} to $\bar{1}, \bar{0}$, respectively). In both cases, $\bar{G}^{(3)} = 1$, by Remark 8.1(b) again. Therefore there is a commutative triangle

$$\begin{array}{ccc} & & G/G^{(3)} \\ & \swarrow & \downarrow \bar{\psi} \\ \bar{G} & \xrightarrow{\ \pi\ } & \mathbb{Z}/p. \end{array}$$

In both cases π is trivial on elements of $\bar{G}$ of order p (for $\bar{G} = M_{p^3}$ this follows from Remark 8.1(c)). The claim follows. ☐

Remark 12.4. Proposition 12.3 is no longer true when $p = 2$. For instance, $G = \mathbb{Z}/2 (\cong G_{\mathbb{R}})$ has Galois relation type, yet $G/G^{(3)} = \mathbb{Z}/2$ and $G^{(2)}/G^{(3)} = 1$. More generally, take $G = G_F$ for a field F of characteristic $\neq 2$. Then $G/G^{(3)}$ contains an involution which is not in $G^{(2)}/G^{(3)}$ if and only if F is formally real [MSp90, Th. 2.7].

Example 12.5. Suppose that $p \neq 2$ and that G has Galois relation type. By Proposition 12.3, $G/G^{(3)}$ cannot be isomorphic to $(\mathbb{Z}/p)^I$, with $I \neq \emptyset$, to H_{p^3}, nor to M_{p^3} (see Remark 8.1(c)).

Remark 12.6. By the celebrated Artin–Schreier theorem, an absolute Galois group of a field is either 1, $\mathbb{Z}/2$, or is infinite. Our results provide a new cohomological proof of this fact in characteristic 0, as follows.

Assume that F is a field of characteristic 0 with $G = G_F$ finite. If $G \cong \mathbb{Z}/p$ with $p \neq 2$, then F contains a primitive pth root of unity. By Proposition 3.2, G has Galois relation type, contrary to what we have seen in Example 12.5. This shows that G is a finite 2-group.

Next suppose that G contains an element of order 4. We may then assume that $G \cong \mathbb{Z}/4$. Let K be its unique subgroup of order 2 and write $H^1(K) = \{0, \psi\}$. The map $\mathrm{res}_K\colon H^1(G) \to H^1(K)$ is trivial. Hence the Kummer element $\kappa_2(-1) \in H^1(K)$ (which comes from $H^1(G)$) is zero. By Corollary 2.8(b), $\beta_K(\psi) = \psi \cup \kappa_2(-1) = 0$. On the other hand, there are no epimorphisms $K \to \mathbb{Z}/4$, contrary to Lemma 10.1.

Hence, G consists of involutions. By Proposition 10.3, $G \cong 1, \mathbb{Z}/2$.

13. Examples

We first give examples showing that non of the groups listed in Corollaries 11.3 and 11.2 can be omitted from these lists.

Example 13.1. Taking $G = G_{\mathbb{C}} = 1$ we see that the trivial group cannot be removed from the above lists.

Example 13.2. For $p = 2$ and $G = G_{\mathbb{R}} = \mathbb{Z}/2$ one has $G^{(3)} = 1$. This shows that $\mathbb{Z}/2$ cannot be removed from the list in Corollary 11.3.

Example 13.3. Let F be a finite field and let $G = G_F = \hat{\mathbb{Z}}$. Then $G/G^{(3)} \cong \mathbb{Z}/p^2$. Therefore $\mathbb{Z}/p^2$ cannot be removed from the lists.

Example 13.4. Take $p = 2$ and $F = \mathbb{R}((t))$. Then $G = G_F = \langle \tau, \epsilon \mid \epsilon^2 = (\tau\epsilon)^2 = 1 \rangle$ [Efr06, §22.1]. There is an epimorphism $G \mapsto D_4$, $\tau \mapsto r$, $\epsilon \mapsto s$ (with notation as in §8). Hence $G/G^{(3)}$ is non-abelian. Now let N_0 be the intersection of all closed normal subgroups N of G such that G/N is isomorphic to one of 1, $\mathbb{Z}/2$,and $\mathbb{Z}/4$. Then G/N_0 is abelian (in fact, it is isomorphic to $(\mathbb{Z}/2)^2$). Consequently, $N_0 \neq G^{(3)}$. Therefore D_4 cannot be removed from the list in Corollary 11.3.

Example 13.5. Let $p \neq 2$. Dirichlet's theorem on primes in arithmetical progressions yields $n \geq 0$ with $l = p(pn+1)+1$ prime. Let ζ_{p^2} be in the algebraic closure of $\mathbb{F}_l$. Then $\mathbb{F}_l$ contains the pth roots of unity, but does not contain a p^2th root of unity ζ_{p^2}. Therefore the maximal pro-p Galois group $G_{\mathbb{F}_l}(p)$ has a generator $\bar{\sigma}$ such that $\bar{\sigma}(\zeta_{p^2}) = \zeta_{p^2}^{1+p}$. Lift $\bar{\sigma}$ to some $\sigma \in G = G_{\mathbb{Q}_l}(p)$. Also let τ be a generator of the inertia group of G. Then G is generated by τ and σ, subject to the defining relation $\sigma\tau\sigma^{-1} = \tau^{1+p}$ [Efr06, Example 22.1.6].

Now let N_0 be the intersection of all closed normal subgroups N of G with G/N isomorphic to 1 or $\mathbb{Z}/p^2$. Then G/N_0 is abelian. Since there is an epimorphism $G \to M_{p^3}$, $\tau \mapsto r$, $\sigma \mapsto s$ (notation as in §8), $G/G^{(3)}$ is non-abelian, so $N_0 \neq G^{(3)}$ (in fact, $G/N_0 \cong (\mathbb{Z}/p^2) \times (\mathbb{Z}/p)$ while $G/G^{(3)} \cong (\mathbb{Z}/p^2) \rtimes (\mathbb{Z}/p^2) = \langle \tilde{\tau} \rangle \rtimes \langle \tilde{\sigma} \rangle$, with action $\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1} = \tilde{\tau}^{1+p}$). Thus M_{p^3} cannot be removed from the list in Corollary 11.2.

Our final two examples show that in Corollaries 11.3 and 11.2 one cannot omit the assumption that G has Galois relation type.

Example 13.6. Let $p = 2$ and let $G = Q_8$. Then G has no normal subgroups N with $G/N \cong \mathbb{Z}/4$ or $G/N \cong D_4$, and has three distinct normal subgroups N with $G/N \cong \mathbb{Z}/2$, all containing the center $Z(G)$.

Thus the intersection of all normal subgroups N of G as in Corollary 11.3 is $Z(G)(\cong \mathbb{Z}/2)$. On the other hand, $G^{(3)} = 1$ (Remark 8.1(b)).

Example 13.7. Let $p \neq 2$ and let $G = \mathbb{Z}/p$ or $G = H_{p^3}$. Then G has no quotients isomorphic to $\mathbb{Z}/p^2$ or M_{p^3}. Thus the intersection in Corollary 11.2 is G itself. But by Remark 8.1(b), $G^{(3)} = 1$.

In this respect, the Main Theorem is a genuine structural result about absolute Galois groups.

Remark 13.8. In view of Corollaries 11.3 and 11.2, the previous two examples show that Q_8 (when $p = 2$) and $\mathbb{Z}/p$, H_{p^3} (when $p \neq 2$) do not have Galois relation type. This can be seen directly as follows.

For $G = Q_8$ and $p = 2$, one has a graded ring isomorphism

$$H^*(Q_8) \cong \mathbb{F}_2[x, y, z]/(x^2 + xy + y^2, x^2y + xy^2),$$

where x, y, z have degrees $1, 1, 4$, respectively (see [Ade97, p. 811, Example], [AM04, Ch. IV, Lemma 2.10]). In this ring, no product of nonzero elements of degree 1 vanishes, yet $x^2 + xy + y^2 = 0$. Hence condition (i) of Definition 3.1 is not satisfied for $G = Q_8$.

For $G = \mathbb{Z}/p$ and $p \neq 2$ one has $H^*(G) \cong \mathbb{F}_p[x, y]/(x^2)$, where x, y have degrees $1, 2$, respectively, and (with the obvious abuse of notation) $\beta_G(x) = y$ [Eve91, §3.2]. Here $\cup\colon H^1(G) \times H^1(G) \to H^2(G)$ is the zero map, but $\beta_G(x) \neq 0$. Hence (ii) of Definition 3.1 is not satisfied.

For $G = H_{p^3}$ and $p \neq 2$, the structure of $H^*(G)$ is considerably more complicated, and was computed by Leary [Lea92, Th. 6 and Th. 7]. Here as well, $\cup\colon H^1(G) \times H^1(G) \to H^2(G)$ is the zero map, but β_G is nontrivial. Therefore condition (ii) of Definition 3.1 is not satisfied.

References

[Ade97] A. Adem, *Recent developments in the cohomology of finite groups*, Notices of the AMS **44** (1997), 806–812.

[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.

[AM04] A. Adem and R. J. Milgram, *Cohomology of Finite Groups*, 2nd ed., Springer-Verlag, Berlin, 2004.

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

[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.

[Bra89] G. Brattström, *On p-groups as Galois groups*, Math. Scand. **65** (1989), 165–174.

[CE56] E. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, 1956.

[Cha82] G. R. Chapman, *The Cohomology Ring of a Finite Abelian Group*, Proc. London Math. Soc. **45** (1982), 564–576.

[Efr06] I. Efrat, *Valuations, Orderings, and Milnor K-theory*, Mathematical Surveys and Monographs, vol. 124, American Mathematical Society, Providence, RI, 2006.

[Eve91] L. Evens, *The Cohomology of Groups*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991.

[Frö85] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. **360** (1985), 84–123.

[GS06] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, Cambridge, 2006.

[Hoe68] K. Hoechsmann, *Zum Einbettungsproblem*, J. reine angew. Math. **229** (1968), 81–106.

[Koc02] H. Koch, *Galois Theory of p-Extensions*, Springer, Berlin, 2002.

[Led05] A. Ledet, *Brauer Type Embedding Problems*, Fields Institute Monographs, vol. 21, American Mathematical Society, Providence, RI, 2005.

[Lea92] I. J. Leary, *The mod-p cohomology rings of some p-groups*, Math. Proc. Camb. Phil. Soc. **112** (1992), 63–75.

[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.

[MN77] R. Massy and T. Nguyen-Quang-Do, *Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3: étude locale-globale*, J. reine angew. Math. **291** (1977), 149–161.

[Mas87] R. Massy, *Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p*, J. Algebra **109** (1987), 508–535.

[MeSu82] 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.

[MS91] J. Mináč and T. L. Smith, *A characterization of C-fields via Galois groups*, J. Algebra **137** (1991), 1–11.

[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.

[NSW00] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, Springer, Berlin, 2000.

[TA85] J.-P. Tignol and S. A. Amitsur, *Kummer subfields of Malcev–Neumann division algebras*, Israel J. Math. **50** (1985), 114–144.

[Tig86] J.-P. Tignol, *Cyclic and elementary abelian subfields of Malcev–Neumann division algebras*, J. Pure Appl. Algebra **42** (1986), 199–220.

[TK88] L. Townsley-Kulich, *Investigations of the integral cohomology ring of a finite group*, Ph.D. thesis, Northwestern University, 1988.

[Vil88] F. R. Villegas, *Relations between quadratic forms and certain Galois extensions*, a manuscript, Ohio State University, 1988, `http://www.math.utexas.edu/users/villegas/osu.pdf`.

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