ANNALES SCIENTIFIQUES DE L'É.N.S.

KAY WINGBERG

On Demuskin groups with involution

Annales scientifiques de l'É.N.S. 4^e série, tome 22, n° 4 (1989), p. 555-567

<http://www.numdam.org/item?id=ASENS_1989_4_22_4_555_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 22, 1989, p. 555 à 567.

ON DEMUSKIN GROUPS WITH INVOLUTION

BY KAY WINGBERG

In algebraic number theory in many situations Poincaré groups occur as Galois groups of p-extensions of local or global fields. Most important are Poincaré groups of dimension two – the so called Demuškin groups – which are characterized by the following properties: A finitely generated pro-p-group G is a Demuškin group if and only if G is an one relator group, *i. e.*,

$$\dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z}) = 1,$$

and the cupproduct

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z})$$

defines a non-degenerating bilinear form.

In order to decide whether a given group G is of this type in practice the first assertion in easier to establish than the second (*e. g.* counting dimensions in a Hochschild Serre spectral sequence if G is given as factor group of a known group). The most common procedure to prove the second is to connect the cupproduct pairing with a known reciprocity law, *i. e.*, a duality theorem, which often involves a lot of difficulties.

The situation becomes much easier if there exists an involution acting on the pro-p-group G, where p is an odd prime number. Then the second assertion can be reduced to an equality of dimensions of certain cohomology groups. This method will be demonstrated in the following example where the equality of dimensions follows easily using Kummer theory.

Let p be an odd prime number and let k be an algebraic number field of CM-type containing the group μ_p of p-th roots of unity, *i. e.*, $k = k^+(\mu_p)$ where k^+ is the maximal totally real subfield of k. Let $k_\infty = k(\mu_{p^\infty})$ be the cyclotomic $\mathbb{Z}_p$-extension of k and we assume that the Iwasawa μ-invariant of k_∞ is equal to zero. This is conjecturally always true and has been proved for abelian extensions $k/\mathbb{Q}$ by Ferrero and Washington. Let $k(p)$ and $k_{S_p}(p)$ be the maximal p-extension and the maximal p-extension unramified outside the set S_p of primes of k above p, respectively.

Now we define a natural p-extension of k which is Galois over k^+ by restricting the ramification at p using the primes at infinity. For every prime $\mathfrak{p} \in S_p(k_\infty)$ we choose a prime $\mathfrak{P}$ in $k(p)$ above $\mathfrak{p}$ and an involution $\rho_\mathfrak{p} \in G(k(p)/k_\infty^+)$ such that

$$\rho_\mathfrak{p} \mathfrak{P} = \mathfrak{P}'$$

where $\mathfrak{P}$ and $\mathfrak{P}'$ are the chosen primes above $\bar{\mathfrak{p}} := \mathfrak{p} \cap \mathcal{O}_{k_\infty^+}$. Hence there are two cases: if $\bar{\mathfrak{p}}$ splits in k_∞, *i.e.*, $\bar{\mathfrak{p}}\mathcal{O}_{k_\infty} = \mathfrak{p}\mathfrak{p}'$, then the involution $\rho_\mathfrak{p}$ interchanges the primes $\mathfrak{P}/\mathfrak{p}$ and $\mathfrak{P}'/\mathfrak{p}'$. Otherwise $\rho_\mathfrak{p}$ is an element in the decomposition group $G_\mathfrak{P}(k(p)/k_\infty^+)$ of $G(k(p)/k_\infty^+)$ with respect to $\mathfrak{P}/\mathfrak{p}$.

Let

$$T_\mathfrak{P}(k(p)/k_\infty^+) \qquad \text{and} \qquad T_{v(\mathfrak{p})}(k(p)/k_\infty^+) = \langle \rho_\mathfrak{p} \rangle$$

be the inertia subgroups of $G(k(p)/k_\infty^+)$ with respect to $\mathfrak{P}/\mathfrak{p}$, $\mathfrak{p} \in S_p(k_\infty)$, and with respect to the prime $v(\mathfrak{p})$ above infinity corresponding to $\rho_\mathfrak{p}$.

We define the maximal p-extension $\tilde{k}$ which is *positively ramified* at p by the closed normal subgroup of $G(k(p)/k_\infty^+)$ generated by the commutator groups $[T_\mathfrak{P}(k(p)/k_\infty^+), T_{v(\mathfrak{p})}(k(p)/k_\infty^+)]$

$$G(k(p)/\tilde{k}) := ([T_\mathfrak{P}(k(p)/k_\infty^+), T_{v(\mathfrak{p})}(k(p)/k_\infty^+)], \mathfrak{p} \in S_p(k_\infty)) \trianglelefteq G(k(p)/k^+).$$

Finally let

$$\tilde{k}_{S_p} = k_{S_p}(p) \cap \tilde{k}$$

be the maximal p-extension of k unramified outside S_p and positively ramified at p.

Let us remark, if all primes of k^+ above p do not split in k then

$$G(k(p)/\tilde{k}) = (T_\mathfrak{P}(k(p)/k^+(p)k), \mathfrak{P}/p) = (G_\mathfrak{P}(k(p)/k^+(p)k), \mathfrak{P}/p),$$

with other words, $\tilde{k}$ is the maximal p-extension of k such that for all completions with respect to primes $\mathfrak{p}$ above p

$$\tilde{k}_\mathfrak{p} \subseteq (k^+(p)k)_\mathfrak{p}.$$

This is just the definition of positively ramified (resp. positively decomposed) extensions used in [7], [8], [9].

THEOREM. — *The Galois group $G(\tilde{k}_{S_p}/k_\infty)$ is a Demuškin group of rank $2g$, where g is equal to the Iwasawa λ-invariant of the minus part of the maximal abelian unramified p-extension of k_∞. More precisely, there exist generators $x_1, y_1, \ldots, x_g, y_g$ of $G(\tilde{k}_{S_p}/k_\infty)$ with one defining relation*

$$\prod_{i=1}^{g} [x_i, y_i] = 1.$$

In order to prove the theorem we use the action of the Galois group $\Delta = G(k/k^+)$ on the pro-p-group $G(\tilde{k}_{S_p}/k_\infty)$ and the general theory developed in the following section. This proof is much easier than the original one and the result is more general since the primes above p are allowed to split in the extension k/k^+ (*see* [7], Theorem).

1. Demuškin groups

Let p be an odd prime number and let Δ be a group of order 2 with generator ρ. For a $\mathbb{Z}_p[\Delta]$ module M we denote by $M^{\pm}$ the direct summands $(1 \pm \rho)M$ of M, hence M^+ is the fix module M^{Δ} of Δ and on M^- the group Δ acts by multiplication with -1.

In the following let G be a pro-p-group with Δ-action, *i. e.*, a Δ-operator group. Then Δ acts on all cohomology groups of G. As usual $H^i(G)$ denotes the i-th cohomology group of G with coefficients $\mathbb{Z}/p$.

LEMMA 1. — *Let* G *be an one-relator group,* i. e., $\dim H^2(G) = 1$, *such that*

$$H^2(G)^+ = 0.$$

Then the following is true:

(i) *If* U *is a* Δ*-invariant subspace of* $H^1(G)$ *which is non-degenerate with respect to the bilinear form given by the cupproduct, then*

$$\dim U^+ = \dim U^-.$$

(ii) *The assertions*

$$\dim H^1(G)^+ = \dim H^1(G)^-$$

and

$$\dim (\operatorname{rad} H^1(G))^+ = \dim (\operatorname{rad} H^1(G))^-$$

are equivalent. Here $\operatorname{rad} H^1(G)$ *denotes the kernel of the cupproduct pairing. In particular,* G *is a Demuškin group if and only if*

$$\dim H^1(G)^+ = \dim H^1(G)^- \quad \textit{and} \quad \operatorname{rad} H^1(G)^+ = 0 \; [\textit{or} \operatorname{rad} H^1(G)^- = 0].$$

Proof: Let $\chi, \chi' \in U$ then

$$\rho\chi \cup \rho\chi' = \rho(\chi \cup \chi') = -\chi \cup \chi'$$

shows that $U^{\pm}$ are totally isotropic subspaces of U. This proves (i). As a consequence we get the equality

$$\dim (H^1(G)/\operatorname{rad} H^1(G))^+ = \dim (H^1(G)/\operatorname{rad} H^1(G))^-$$

which implies (ii) [observe that rad $H^1(G)$ is a Δ-invariant summand of $H^1(G)$].

Now let

$$G^- := (G^{1-\rho}) \leqq G$$

be the closed normal subgroup of G generated by all elements $gg^{-\rho}$, $g \in G$, and let

$$G^+ := G/G^-.$$

We define

$$\mathscr{A} := \{ N \trianglelefteq G \text{ open, normal} \mid G^- \leqq N \}$$

to be the set of all open normal subgroups of G containing G^-, with other words $\mathscr{A}$ is the set of the full pre-images of open normal subgroups of G^+ with respect to the canonical surjection $G \twoheadrightarrow G^+$. Furthermore let

$$\mathscr{A}_p := \{ N \in \mathscr{A} \mid (G:N) \leqq p \}.$$

Observe that Δ acts on all $N \in \mathscr{A}$: $n^\rho = n(n^{-1} n^\rho) \in N$ for $n \in N$. Obviously for $N \in \mathscr{A}$ there is a canonical isomorphism

$$H^1(N^+) \underset{\text{inf}}{\xrightarrow{\sim}} H^1(N)^+$$

given by the inflation map. Furthermore we have

$$N^- = G^- \quad \text{resp.} \quad N^+ = N/G^-.$$

Indeed, let $g, \bar{g} \in G$ then

$$\bar{g}^{(1-\rho)g^2} = n^{(1-\rho)g}$$

where

$$n = \bar{g}^{(1-\rho)} \in G^- \subseteq N.$$

Hence

$$G^- = N^-[N, G^-]$$

showing the assertion above as N is pro-nilpotent.

Since there is an equivalence of categories between the prop-p Δ-operator groups and the split group extensions of Δ by pro-p-groups together with a section, we obtain for $N \in \mathscr{A}$ an open normal subgroup $\mathscr{N}$ of $\mathscr{G}$, where $\mathscr{G}$ is the semi direct product of Δ and the Δ-group G, *i. e.*, there is a commutative and exact diagram

$$\begin{array}{ccccccccc} 1 & \to & G & \to & \mathscr{G} & \overset{s}{\underset{\leftarrow}{\rightarrow}} & \Delta & \to & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 1 & \to & N & \to & \mathscr{N} & \overset{s}{\underset{\leftarrow}{\rightarrow}} & \Delta & \to & 1. \end{array}$$

Obviously we have

$$H^i(\mathscr{N}) \underset{\text{res}}{\xrightarrow{\sim}} H^i(N)^\Delta \quad \text{for all } i \geqq 0.$$

LEMMA 2. — *There is a canonical isomorphism*

$$G^+ \xrightarrow{\sim} \mathscr{G}(p)$$

from G^+ *on the maximal pro-p-factor group* $\mathcal{G}(p)$ *of* $\mathcal{G}$. *Furthermore* G^+ *is a free pro-p-group if* $H^2(G)^+ = 0$.

Proof: Consider the exact and commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & I \cap G & \to & I & \overset{s}{\underset{\leftarrow}{\rightleftarrows}} & \Delta & \to & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \to & G & \to & \mathcal{G} & \overset{s}{\underset{\leftarrow}{\rightleftarrows}} & \Delta & \to & 1 \\ & & \downarrow & & \downarrow & & & & \\ & & \tilde{G} & \twoheadrightarrow & \mathcal{G}(p) & & & & \end{array}$$

where I is the kernel of the canonical surjection $\mathcal{G} \twoheadrightarrow \mathcal{G}(p)$ and $\tilde{G}$ denotes the factor group $G/I \cap G$.

Since Δ acts on $I \cap G$ via s we obtain on $\tilde{G}$ a Δ-action induced by the Δ-operator group G. But this action is trivial.

$$g^{s(\rho)-1} = [s(\rho), g] \in I \cap G \qquad \text{for} \quad g \in G,$$

implying that there is a surjection

$$\varphi: \quad G^+ \twoheadrightarrow \tilde{G}.$$

Now we obtain an exact and commutative diagram using the Hochschild-Serre spectral sequence

$$\begin{array}{ccccccccc} 0 \to & H^1(\tilde{G}) & \to H^1(G^+) & \to H^1(\ker\varphi)^{G^+} \to & H^2(\tilde{G}) & \to H^2(G^+) \\ & \overset{\text{res}}{\uparrow} \cong & \underset{\cong}{\downarrow}\,\text{inf} & & \overset{\text{res}}{\uparrow} \cong & \underset{\cong}{\downarrow}\,\text{inf} \\ & H^1(\mathcal{G}(p)) & \twoheadrightarrow H^1(\mathcal{G}) & & H^1(\mathcal{G}(p)) & \underset{\text{inf}_2}{\hookrightarrow} H^2(\mathcal{G}) \end{array} \qquad \begin{array}{c} \\ H^1(G)^+ \\ \cong \uparrow \text{res} \\ \\ H^2(G)^+ \\ \cong \uparrow \text{res} \\ \\ \end{array}$$

[Hom $(I, \mathbb{Z}/p) = 0$ implies the injectivity of inf_2] showing $H^1(\ker\varphi)^{G^+} = 0$ thus $\ker\varphi = 0$.

We introduce some further notations. Let G be an one-relator group and

$$\dim H^1(G) = n$$
$$G^{ab} \cong \mathbb{Z}_p^{n-1} \times \mathbb{Z}_p/p^s\mathbb{Z}_p$$

where $1 \leqq s \leqq \infty$ $(p^\infty = 0)$. If s is finite let B be the Bockstein operator, *i.e.*, the δ-homomorphism

$$H^1(G, \mathbb{Z}/p^s) \overset{B}{\twoheadrightarrow} H^2(G, \mathbb{Z}/p^s) \cong \mathbb{Z}/p^s$$

induced by the exact sequence

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

Hence we obtain an exact sequence

$$0 \to {}_p\mathrm{Ker}\, B \to H^1(G) \xrightarrow{\delta} H^2(G) \to 0$$

where δ is defined by B restricted to ${}_pH^1(G, \mathbb{Z}/p^s) \cong H^1(G)$ and ${}_pM$ denotes the subgroup $\{x \in M \mid px = 0\}$ of an abelian group M. Furthermore let m be the (even) integer

$$m = n - \dim \mathrm{rad}\, H^1(G).$$

LEMMA 3. — *Let* G *be an one relator group with* Δ*-action such that*

$$H^2(G)^+ = 0,$$
$$\dim H^1(G)^+ = \dim H^1(G)^-.$$

Then there exists a basis $\chi_1, \ldots, \chi_n$ *of* $H^1(G)$ *such that*

(*a*) $H^1(G)^\pm = \{\chi_i \mid i^{\mathrm{odd}}_{\mathrm{even}}\}$

(*b*) $\chi_1 \cup \chi_2 = \chi_3 \cup \chi_4 = \ldots = \chi_{m-1} \cup \chi_m = 1$

$$\chi_i \cup \chi_j = 0 \text{ for all other pairs } (i,j) \text{ with } i < j.$$

(*c*) *If s is finite then*

$$\delta\chi_{i_0} = 1 \quad \text{and} \quad \delta\chi_i = 0 \quad \text{for } i \neq i_0$$

where

$$i_0 = \begin{cases} 1, & \text{if } {}_p\ker B \supseteq \mathrm{rad}\, H^1(G) \\ m+1, & \text{if } {}_p\ker B \not\supseteq \mathrm{rad}\, H^1(G) \end{cases}.$$

Proof. — Since $H^1(G)^\pm$ are totally isotropic subspaces of $H^1(G)$ it is obvious that a basis of $H^1(G)$ exists satisfying (*a*) and (*b*). If s is finite then there exists $\chi_{i_0} \in H^1(G)$ such that $\delta\chi_{i_0} \neq 0$ where i_0 is odd, because $H^2(G) = H^2(G)^-$. We may assume that $\delta\chi_{i_0} = 1$ and that after permutation i_0 is given as in (*c*). Replacing for i odd and not equal to i_0 the character χ_i by

$$\chi_i - (\delta\chi_i)\chi_{i_0} \in H^1(G)^-$$

then $\delta\chi_i = 0$ for $i \neq i_0$. Finally we make the substitution

$$\chi_2 - \sum_{i=4,6,\ldots,m} (\chi_{i-1} \cup \chi_2)\chi_i \in H^1(G)^+$$

for χ_2 obtaining a basis with the desired properties.

Now a result of Dummit and Labute [1] allows us to prove the main result of this section:

THEOREM 1. — *Let* G *be a finitely generated one-relator pro-p-group, where p is an odd prime number. Suppose that* G *admits an action of a group* Δ *of order* 2 *such that*

$H^2(G)^\Delta = 0$. *Then the following assertions are equivalent:*

(i) G *is a Demuškin group.*

(ii) $\dim H^1(N)^+ = \dim H^1(N)^-$ *for all* $N \in \mathscr{A}_p$.

Proof. — If G is a Demuškin group then all open subgroups of G are Demuškin groups (*cf.* [5]) and in particular all $N \in \mathscr{A}_p$. Furthermore in this case the corestriction map

$$H^2(N) \underset{\text{cor}}{\rightarrow} H^2(G)$$

is an isomorphism showing $H^2(N)^\Delta = 0$. Now Lemma 1 (iii) implies assertion (ii).

Conversely assume that (ii) is fulfilled. We choose a basis $\{\chi_1, \ldots, \chi_n\}$ of $H^1(G)$ with the properties of Lemma 3. Let

$$1 \to R \to F \to G \to 1$$

be a minimal presentation of G by a free pro-p-group F of rank n and a closed normal subgroup $R = \langle r \rangle$ of F generated by $r \in F$. If $\{x_i \bmod F^p[F, F]\}$ is a dual basis of the basis $\{x_i\}$ of $H^1(F) = H^1(G)$ then

$$r \equiv \prod_{i=1}^{n} x_i^{a_i p^s} \cdot [x_1, x_2] \ldots [x_{m-1}, x_m] \bmod [F, F]^p [F, [F, F]]$$

where $a_i \in \mathbb{Z}_p$, $a_{i_0} \equiv 1 \bmod p$ and $a_i \equiv 0 \bmod p$ for $i \neq i_0$.

Replacing x_{i_0} by $\prod_{i=1}^{n} x_i^{-a_i/a_{i_0}}$ we may assume that $a_{i_0} = 1$ and $a_i = 0$ for $i \neq i_0$.

Now suppose that the cupproduct is degenerated, *i.e.*, $m < n$, then the open normal subgroup

$$E := \langle x_n^p, x_i^{x_n^j}, 1 \leqq i \leqq n-1, 0 \leqq j \leqq p-1 \rangle$$

of F is of index p and

$$N := E/R$$

is an open normal subgroup of G of index p.

Since

$$H^1(G/N) = \langle \chi_n \rangle \subseteq H^1(G)^+$$

N is contained in $\mathscr{A}_p$. Observing that G^+ is free (Lemma 2), and that $N^+ = N/G^-$ has index p in G^+ our assumption (ii) leads to the equality

$$\begin{aligned} \dim H^1(N) - 2 &= 2 \dim H^1(N)^+ - 2 \\ &= 2p(\dim H^1(G)^+ - 1) \\ &= p(\dim H^1(G) - 2). \end{aligned}$$

But by the result of Dummit and Labute one obtains for this group N

$$\dim H^1(N) > 2 + p(\dim H^1(G) - 2).$$

Therefore G has to be a Demuškin group.

2 Application to global number fields

For the algebraic number field k of CM-type containing μ_p, p odd, let the fields k^+, k_∞, $k(p)$, k_{S_p} and $\tilde{k}_{S_p}$ be defined as in the introduction. Let

$$T_p = \underset{\mathfrak{P} \mid p}{*} T_{\mathfrak{P}}(k(p)/k_\infty)$$

be the free pro-p-product of all inertia subgroups of $G(k(p)/k_\infty)$ with respect to the primes $\mathfrak{P}$ above p. [The index set $\mathfrak{P}|p$ of the free pro-p-product is the projective limit of the finite sets $S_p(K)$ provided with the cofinal topology where K/k runs through all finite Galois p-extensions of k_∞.] The Galois group $G(k(p)/k_\infty)$ acts on T_p continuously by conjugation: every $\sigma \in G(k(p)/k_\infty)$ defines an automorphism of T_p induced by the isomorphisms

$$T_{\mathfrak{P}}(k(p)/k_\infty) \xrightarrow{\sim} T_{\sigma\mathfrak{P}}(k(p)/k_\infty), \qquad x \mapsto x^{\sigma^{-1}}.$$

Let $G = G(k(p)/k_\infty)$ and $G_{\mathfrak{P}} = G_{\mathfrak{P}}(k(p)/k_\infty)$. The canonical surjection

$$\varphi: \quad T_p = \underset{\mathfrak{p} \in S_p(k_\infty)}{*} \; \underset{\sigma \in G/G_{\mathfrak{P}}}{*} T_{\sigma\mathfrak{P}}(k(p)/k_\infty) \twoheadrightarrow \underset{\bar{\mathfrak{p}} \in S_p(k_\infty^+)}{*} \; \underset{\sigma \in G/G_{\mathfrak{P}}}{*} T_{\overline{\sigma\mathfrak{P}}}(k^+(p)/k_\infty^+) =: T_p(+)$$

is defined by the maps

$$\varphi_{\sigma\mathfrak{P}}: \quad T_{\sigma\mathfrak{P}}(k(p)/k_\infty) \twoheadrightarrow T_{\widetilde{\sigma\mathfrak{P}}}(k^+(p)k/k_\infty) \xrightarrow{\sim} T_{\overline{\sigma\mathfrak{P}}}(k^+(p)/k_\infty^+)$$

where $\widetilde{\sigma\mathfrak{P}}$ and $\overline{\sigma\mathfrak{P}}$ are the underlying primes of $\sigma\mathfrak{P}$ in $k^+(p)k$ and $k^+(p)$, respectively.

We have

$$\ker \varphi_{\sigma\mathfrak{P}} = T_{\sigma\mathfrak{P}}(k(p)/k^+(p)k)$$

and this group is trivial if the underlying prime $\bar{\mathfrak{p}}$ of k_∞^+ splits in k_∞ by the Theorem of Grunwald-Hasse-Wang (*see* [4], proof of Theorem 11.3):

$$\begin{aligned} G_{\sigma\mathfrak{P}}(k(p)/k^+(p)k) &\cong G(k(p)_{\bar{\mathfrak{p}}}/(k^+(p)k)_{\bar{\mathfrak{p}}}) \\ &\cong G(k_{\bar{\mathfrak{p}}}(p)/k_{\bar{\mathfrak{p}}}^+(p)k_{\bar{\mathfrak{p}}}) = 1 \end{aligned}$$

because the completions $k_{\bar{\mathfrak{p}}}$ and $k_{\bar{\mathfrak{p}}}^+$ are equal.

If the underlying prime does not split in k_∞ we have

$$T_{\sigma\mathfrak{P}}(k(p)/k^+(p)k) = (T_{\sigma\mathfrak{P}}(k(p)/k_\infty)^{1-\rho_{\bar{\mathfrak{p}}}^{\sigma^{-1}}})_{T_{\sigma\mathfrak{P}}(k(p)/k_\infty)}$$

since $T_{\sigma\mathscr{P}}(k^+(p)k/k_\infty)$ is the maximal quotient of $T_{\sigma\mathscr{P}}(k(p)/k_\infty)$ on which $\rho_{\mathfrak{p}}^{\sigma^{-1}}$ acts trivially.

Therefore

$$T_p(-) := \ker\varphi = \langle T_{\sigma\mathscr{P}}(k(p)/k_\infty)^{1-\rho_{\mathfrak{P}}^{\sigma^{-1}}},\ \mathfrak{p}\in S_p(k_\infty),\ \sigma\in G(k(p)/k_\infty)\rangle.$$

Let ψ be the canonical map from T_p in $G(k(p)/k_\infty)$ given by the injections

$$\psi_{\sigma\mathscr{P}}:\quad T_{\sigma\mathscr{P}}(k(p)/k_\infty) \subsetneq G(k(p)/k_\infty).$$

As $T_p(-)$ is a $G(k(p)/k_\infty)$-operator group its image under ψ is normal in $G(k(p)/k_\infty)$ and defines the field $\tilde{k}$:

$$\psi(T_p(-)) = ([T_{\mathscr{P}}(k(p)/k_\infty^+), T_{v(\mathfrak{p})}(k(p)/k_\infty^+)], \mathfrak{p}\in S_p(k_\infty))_{G(k(p)/k_\infty)}.$$

Therefore we obtain the commutative and exact diagram

$$\begin{array}{ccccccc} 1\to & T_p(-) & \to & T_p & \to T_p(+)\to 1 \\ & \downarrow\psi & & \downarrow\psi & \\ 1\to & \psi(T_p(-)) & \to & G(k(p)/k_\infty) & \to G(\tilde{k}/k_\infty)\to 1. \end{array}$$

LEMMA 1. — *Local class field theory implies an exact and commutative diagram*

$$\begin{array}{ccccccccc} 0\to & H^1(T_p(+),\mathbb{Q}_p/\mathbb{Z}_p)^G & \to & H^1(T_p,\mathbb{Q}_p/\mathbb{Z}_p)^G & \to & H^1(T_p(-),\mathbb{Q}_p/\mathbb{Z}_p)^G & \to 0 \\ & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & \\ 0\to & (U_\infty^+)^* & \to & (U_\infty)^* & \to & (U_\infty^-)^* & \to 0 \end{array}$$

where

$$G = G(k(p)/k_\infty) \qquad \textit{and} \qquad U_\infty = U(k_\infty) = \prod_{\mathfrak{p}\in S_p(k_\infty)} \varprojlim_n U^1((k_n)_{\mathfrak{p}})$$

is the projective limit with respect to the norm maps of the local principal units of the n-th layer $(k_n)_{\mathfrak{p}}$ of the local $\mathbb{Z}_p$-extension $(k_\infty)_{\mathfrak{p}}/k_{\mathfrak{p}}$.

Proof. — Since the G-operator group $T_p(+)$ has cohomological dimension 1 the Hochschild-Serre spectral sequence yields an exact sequence

$$\begin{aligned} 0\to H^1(T_p(+))^G \to H^1(T_p)^G \to H^1(T_p(-))^G \\ \to H^1(G, H^1(T_p(+))) \to H^1(G, H^1(T_p)); \end{aligned}$$

here we use for shortness: $H^i(G) := H^i(G,\mathbb{Q}_p/\mathbb{Z}_p)$. Since

$$H^1(T_p) = \prod_{\mathfrak{p}\in S_p(k_\infty)} \mathrm{Ind}_{G_{\mathscr{P}}}^G H^1(T_{\mathscr{P}}(k(p)/k_\infty)),$$

[3] Satz 4.1, we obtain setting $T_{\mathfrak{P}} = T_{\mathfrak{P}}(k(p)/k_\infty)$

$$H^1(G, H^1(T_p)) = \prod_{\mathfrak{p} \in S_p(k_\infty)} H^1(G_{\mathfrak{P}}, H^1(T_{\mathfrak{P}})) = \prod_{\mathfrak{p} \in S_p(k_\infty)} H^1(T_{\mathfrak{P}}, H^1(T_{\mathfrak{P}}))^{G_{\mathfrak{P}}}$$

as

$$H^1(G_{\mathfrak{P}}/T_{\mathfrak{P}}, H^1(T_{\mathfrak{P}})) \cong H^2(G_{\mathfrak{P}}) = 0.$$

But the map

$$\prod_{\bar{\mathfrak{p}} \in S_p(k_\infty^+)} H^1(T_{\mathfrak{P}}, H^1(T_{\bar{\mathfrak{P}}}(k^+(p)/k_\infty^+)))^{G_{\mathfrak{P}}} \to \prod_{\mathfrak{p} \in S_p(k_\infty)} H^1(T_{\mathfrak{P}}, H^1(T_{\mathfrak{P}}))^{G_{\mathfrak{P}}}$$

is injective (observe that this map is diagonal for primes splitting in k_∞/k_∞^+ and that $H^1(T_{\bar{\mathfrak{P}}}(k^+(p)/k_\infty^+)) \subsetneq H^1(T_{\mathfrak{P}})$ is an injection of trivial $T_{\mathfrak{P}}$-modules).

Therefore

$$H^1(G, H^1(T_p(+))) \subsetneq H^1(G, H^1(T_p))$$

is injective. Furthermore

$$H^1(T_p(+))^G = \prod_{\bar{\mathfrak{p}} \in S_p(k_\infty^+)} (\mathrm{Ind}_{G_{\mathfrak{P}}}^G H^1(T_{\bar{\mathfrak{P}}}(k^+(p)/k_\infty^+)))^G = \prod_{\bar{\mathfrak{p}} \in S_p(k_\infty^+)} H^1(T_{\bar{\mathfrak{P}}}(k^+(p)/k_\infty^+))^{G_{\bar{\mathfrak{P}}}}$$

which by local class field theory is isomorphic to $U(k_\infty^+)^*$. Analogous we obtain

$$H^1(T_p)^G = U(k_\infty)^*.$$

This finishes the proof of Lemma 1.

From the surjection

$$T_p(-) \twoheadrightarrow G(k(p)/\tilde{k}) \twoheadrightarrow G(k_{S_p}(p)/\tilde{k}_{S_p})$$

we obtain an injection

$$H^1(G(k_{S_p}(p)/\tilde{k}_{S_p}), \mathbb{Q}_p/\mathbb{Z}_p)^{G(k(p)/k_\infty)} \subsetneq (U_\infty^-)^*$$

resp. a surjection

$$U_\infty^- \twoheadrightarrow G(k_{S_p}(p)/\tilde{k}_{S_p})/[G(k_{S_p}(p)/\tilde{k}_{S_p}), G(k_{S_p}(p)/k_\infty)],$$

and therefore a commutative and exact diagram

$$\begin{array}{ccccccccc} 0 \to & \bar{\mathrm{E}}_\infty & \to \mathrm{U}_\infty & \to \mathrm{G}(k_{\mathrm{S}_p}(p)/k_\infty)^{ab} & \to & \mathrm{G}(\mathrm{L}/k_\infty)^{ab} & \to 0 \\ & & \uparrow & \| & & \uparrow & \\ & & \mathrm{U}_\infty^- & \xrightarrow{\chi} \mathrm{G}(k_{\mathrm{S}_p}(p)/k_\infty)^{ab} & \to & \mathrm{G}(\tilde{k}_{\mathrm{S}_p}/k_\infty)^{ab} & \to 0 \end{array}$$

where L is the maximal unramified p-extension of k_∞ and

$$\bar{\mathrm{E}}_\infty = \varprojlim_n \overline{\mathrm{E}(k_n)}$$

is the projective limit with respect to the norm maps of the topological closure $\overline{\mathrm{E}(k_n)}$ of the image of the global units $\mathrm{E}(k_n)$ in the local groups $\prod_{\mathfrak{p} \mid p} \mathrm{U}^1((k_n)_\mathfrak{p})$ via the diagonal mapping. The upper sequence is exact by class field theory.

The diagram implies isomorphisms

$$(\mathrm{G}(\tilde{k}_{\mathrm{S}_p}/k_\infty)^{ab})^+ \cong \mathrm{G}(k_{\mathrm{S}_p}^+/k_\infty^+)^{ab}$$
$$(\mathrm{G}(\tilde{k}_{\mathrm{S}_p}/k_\infty)^{ab})^- \cong \mathrm{G}(\mathrm{L}/k_\infty)^{ab-}$$

hence

$$\ker \chi = \bar{\mathrm{E}}_\infty^- = \mathbb{Z}_p(1),$$

[6] Theorem 8.17.

Dualizing the lower exact sequence in the diagram above and observing that the weak Leopoldt conjecture holds true for the cyclotomic $\mathbb{Z}_p$-extension, *i.e.*,

$$\mathrm{H}^2(\mathrm{G}(k_{\mathrm{S}_p}(p)/k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0,$$

leads to an exact and commutative diagram

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ \mathrm{H}^1(\mathrm{G}(\tilde{k}_{\mathrm{S}_p}/k_\infty)) & = & (\mathrm{G}(\tilde{k}_{\mathrm{S}_p}/k_\infty)^{ab})^* \\ \downarrow & & \downarrow \\ \mathrm{H}^1(\mathrm{G}(k_{\mathrm{S}_p}(p)/k_\infty)) & = & (\mathrm{G}(k_{\mathrm{S}_p}(p)/k_\infty)^{ab})^* \\ \downarrow & & \downarrow \\ \mathrm{H}^1(\mathrm{G}(k_{\mathrm{S}_p}(p)/\tilde{k}_{\mathrm{S}_p}))^{\mathrm{G}} & \hookrightarrow & (\mathrm{U}_\infty^-)^* \\ \downarrow & & \downarrow \\ \mathrm{H}^2(\mathrm{G}(\tilde{k}_{\mathrm{S}_p}/k_\infty)) & \hookrightarrow & \mathbb{Z}_p(1)^* \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array}$$

Hence we obtain an injection

$${}_p\mathrm{H}^2(\mathrm{G}(\tilde{k}_{\mathrm{S}_p}/k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) \hookrightarrow \mathbb{Z}/p\mathbb{Z}(-1).$$

LEMMA 2. — *Let* K *be a* CM*-field with maximal totally real subfield* K^+ *and let* K_∞ *be the cyclotomic* $\mathbb{Z}_p$*-extension of* K. *Let* $A_\infty = \varinjlim A(K_n)$ *be the direct limit of the p-primary parts of the ideal class groups* $A(K_n)$ *of* K_n *with respect to the maps induced by the inclusions. Then we have a natural isomorphism*

$$G(K_{S_p}^+(p)/K_\infty^+)^{ab} \cong \mathrm{Hom}(A_\infty^-, \mathbb{Q}_p/\mathbb{Z}_p(1)).$$

Proof. — Iwasawa [2], § 7: By Kummer theory there is an exact sequence

$$0 \to E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Hom}(G(K_{S_p}(p)/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p(1)) \to A_\infty \to 0.$$

Since K_∞ is a CM-field we have

$$(E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^- = 0$$

showing the desired result.

From now on we assume that the Iwasawa μ-invariant is zero:

$$\mu(G(k_{S_p}/k_\infty)^{ab}) = 0.$$

This assertion is stable under p-extension, see for example [6], Prop. 7.1. Then

$$G(\tilde{k}_{S_p}/k_\infty)^{ab} \cong G(k_{S_p}^+(p)/k_\infty^+)^{ab} \oplus G(L/k_\infty)^{ab-}$$

is $\mathbb{Z}_p$-torsion free and finitely generated. Hence

$$H^2(G(\tilde{k}_{S_p}/k_\infty), \mathbb{Z}/p\mathbb{Z}) = {}_pH^2(G(\tilde{k}_{S_p}/k_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \subsetneq \mathbb{Z}/p\mathbb{Z}(-1)$$

showing that

$$H^2(G(\tilde{k}_{S_p}/k_\infty), \mathbb{Z}/p\mathbb{Z})^+ = 0.$$

According to Lemma 1.2 the pro-p-group $G(\tilde{k}_{S_p}/k_\infty)^+ = G(k_{S_p}^+(p)\,k/k_\infty)$ is free ($G(\tilde{k}_{S_p}/k_\infty)^+$ is defined by an arbitrary splitting of $G(\tilde{k}_{S_p}/k_\infty^+) \twoheadrightarrow \Delta$).

Now let K_∞ be a finite Galois extension of k_∞ of CM-type inside $\tilde{k}_{S_p}$, *i.e.*, K_∞ is contained in $k_{S_p}^+(p)\,k$. Then there exists an extension K/k_n, n sufficiently large, such that $K_\infty = K\,k_\infty$. Obviously we have for the CM-field $K = K^+(\mu_p)$

$$\tilde{K}_{S_p} = \tilde{k}_{S_p} \qquad \text{and} \qquad K_{S_p}^+(p) = k_{S_p}^+(p).$$

Since the μ-invariant with respect to K_∞ is also zero it follows from Lemma 2

$$\begin{aligned}
\dim H^1(G(\tilde{k}_{S_p}/K_\infty), \mathbb{Z}/p\mathbb{Z})^+ &= \dim H^1(G(k_{S_p}^+(p)/K_\infty^+), \mathbb{Z}/p\mathbb{Z}) \\
&= \mathrm{corank}_{\mathbb{Z}_p} H^1(G(k_{S_p}^+(p)/K_\infty^+), \mathbb{Q}_p/\mathbb{Z}_p) \\
&= \mathrm{corank}_{\mathbb{Z}_p} H^1(G(L_K/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)^- \\
&= \dim H^1(G(L_K/K_\infty), \mathbb{Z}/p\mathbb{Z})^- \\
&= \dim H^1(G(\tilde{k}_{S_p}/K_\infty), \mathbb{Z}/p\mathbb{Z})^-
\end{aligned}$$

Here L_K denotes the maximal unramified p-extension of K_∞. As $G(k_{S_p}^+(p)k/k_\infty)$ is a finitely generated free pro-p-group we obtain

$$\dim H^1(G(\tilde{k}_{S_p}/K_\infty), \mathbb{Z}/p\mathbb{Z}) = [K_\infty : k_\infty](2 \dim H^1(G(\tilde{k}_{S_p}/k_\infty), \mathbb{Z}/p\mathbb{Z}) - 2)$$

showing that $G(\tilde{k}_{S_p}/k_\infty)$ can not be free.

Hence

$$H^2(G(\tilde{k}_{S_p}/k_\infty), \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}(-1).$$

Now Theorem 1 implies the theorem in the introduction.

REFERENCES

[1] D. DUMMIT and J. LABUTE, *On a new Characterization of Demuškin Groups* (*Invent. Math.*, Vol. 73, 1983, pp. 413-418).

[2] K. IWASAWA, *On $\mathbb{Z}_l$-extensions of Algebraic Number fields* (*Ann. of Math.*, Vol. 98, 1973, pp. 246-326).

[3] J. NEUKIRCH, *Freie Produkte pro-endlicher Gruppen und ihre Kohomologie* (*Archiv der Math.*, Vol. 22, 1971, pp. 337-357).

[4] J. NEUKIRCH, *Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen* (*J. reine u. angew. Math.*, Vol. 259, 1973, pp. 1-47).

[5] J.-P. SERRE, *Structures de certains pro-p-groupes* (*Sém. Bourbaki*, No. 252, 1962-1963, pp. 1-11).

[6] K. WINGBERG, *Duality theorems for Γ-extensions of Algebraic Number Fields* (*Compositio Math.*, Vol. 55, 1985, pp. 333-381).

[7] K. WINGBERG, *Ein Analogon zur Fundamentalgruppe einer Riemann'schen Fläche im Zahlkörperfall* (*Invent. Math.*, Vol. 77, 1984, pp. 557-584).

[8] K. WINGBERG, *Positiv-zerlegte p-Erweiterungen algebraischer Zahlkörper* (*J. reine u. angew. Math.*, Vol. 357, 1985, pp. 193-204).

[9] K. WINGBERG, *Galois groups of Poincaré-type over Algebraic Number Fields*, in: Y. IHARA, K. RIBET, J.-P. SERRE, Galois Groups over $\mathbb{Q}$, Springer, New York, 1989.

(Manuscript received April 21, 1988,
in revised form April 24, 1989).

K. WINGBERG,
Universität Erlangen-Nürnberg,
Mathematisches Institut,
Bismarckstrasse 1 1/2,
D-8520 Erlangen,
Federal Republic of Germany.