Free Product Decomposition of Galois Groups of Number Fields

by Kay Wingberg at Heidelberg

Let $G(k(\mathfrak{c})|k)$ be the Galois group of the maximal pro-$\mathfrak{c}$ extension $k(\mathfrak{c})$ of a number field k, where $\mathfrak{c}$ is a full class of finite groups which is closed under taking subgroups, quotients and extensions. If $\mathfrak{p}$ is a prime of k and $\mathfrak{P}$ an extension of $\mathfrak{p}$ to $k(\mathfrak{c})$, then the decomposition group $G_{\mathfrak{P}}(k(\mathfrak{c})|k)$ with respect to $\mathfrak{P}$ is isomorphic to the Galois group $G(k_{\mathfrak{p}}(\mathfrak{c})|k_{\mathfrak{p}})$ of the maximal pro-$\mathfrak{c}$ extension $k_{\mathfrak{p}}(\mathfrak{c})$ of $k_{\mathfrak{p}}$, cf. [4] theorem (9.3.1). In this paper we consider the question whether the decomposition groups $G_{\mathfrak{P}}(k(\mathfrak{c})|k)$ or the inertia groups $T_{\mathfrak{P}}(k(\mathfrak{c})|k)$ for some primes $\mathfrak{p}$ form a free pro-$\mathfrak{c}$-product inside $G(k(\mathfrak{c})|k)$. More precisely, if $S(k)$ and $T_0(k)$ are sets of primes of k, then

$k_S(\mathfrak{c})$	is the maximal pro-$\mathfrak{c}$ extension which is unramified outside S,
$k^{T_0}(\mathfrak{c})$	is the maximal pro-$\mathfrak{c}$ extension which is completely decomposed at T_0,

and we have canonical homomorphisms

$$\phi_S(\mathfrak{c}) : \mathop{\ast}_{\mathfrak{p}\notin S(k_S(\mathfrak{c}))} T_{\mathfrak{P}}(k(\mathfrak{c})|k) \longrightarrow G(k(\mathfrak{c})|k_S(\mathfrak{c})),$$

of the free pro-$\mathfrak{c}$-product of the groups $T_{\mathfrak{P}}(k(\mathfrak{c})|k)$ into $G(k(\mathfrak{c})|k_S(\mathfrak{c}))$ and, if T_0 is finite,

$$\phi^{T_0}(\mathfrak{c}) : \mathop{\ast}_{\mathfrak{p}\in T_0(k^{T_0}(\mathfrak{c}))} G_{\mathfrak{P}}(k(\mathfrak{c})|k) \longrightarrow G(k(\mathfrak{c})|k^{T_0}(\mathfrak{c})),$$

of the free pro-$\mathfrak{c}$-products of the groups $T_{\mathfrak{P}}(k(\mathfrak{c})|k)$ and $G_{\mathfrak{P}}(k(\mathfrak{c})|k)$, respectively; here the prime $\mathfrak{P}$ is a fixed extensions of $\mathfrak{p}$ to $k(\mathfrak{c})$. It is known that the answer of the questions, whether $\phi_S(\mathfrak{c})$ or $\phi^{T_0}(\mathfrak{c})$ are isomorphisms, do not depend on the choice of the extensions $\mathfrak{P}|\mathfrak{p}$ if $\mathfrak{c}$ is the class of finite p-groups, p a prime number, but in general it does, see [4] chap.IV §2. Observe further that in general the sets $S(k_S(\mathfrak{c}))$ (resp. its complement) and $T_0(k^{T_0}(\mathfrak{c}))$ are infinite, and we recall the

Communicated by A.Tamagawa. Received July 22, 2003.
2000 Mathematics Subject Classifications: 11R32, 11R34, 20E18.
Mathematisches Institut, Universität Heidelberg
Im Neuenheimer Feld 288, 69120 Heidelberg, Germany

definition of free profinite products over profinite spaces in section 1 (see [4]). Let us collect some known results.

If $\mathfrak{c}$ is the class of finite p-groups and $S(k)$ is an arbitrary set containing the set $S_p(k)$ of primes above p, then ϕ_S is an isomorphism, see [4] theorem (10.5.1) for the case that p is odd or $S(k)$ contains the set $S_{\mathbb{R}}$ of real places of k and [6] theorem 2 in the remaining case.

If $\mathfrak{c}$ is the class of all finite groups (and $T_0(k)$ is finite), then there exist suitable extensions $\mathfrak{P}|\mathfrak{p}$ such that ϕ^{T_0} is an isomorphism of profinite groups. If $T_0 = S_\infty$ is the set archimedean primes, this is a result of Fried-Haran-Völklein [1] and in general it is proven by Pop [5].

We also would like to mention a result of Neukirch, [3] Satz (12.2), which says that *finitely many* decomposition groups $G_{\mathfrak{P}}(k(p)|k)$ form a free pro-p-product inside $G(k(p)|k)$.

In this paper we will prove that $\phi^{T_0}(\mathfrak{c})$ is an isomorphism if $\mathfrak{c}$ is the class of finite p-groups. We get even more: let S, T_0 be sets of primes of k such that $S_p \cup S_\infty \subset S$, the density $\delta(S)$ of S is equal to 1 and T_0 is a finite subset of S and let

$k_S^{T_0}(p)$ be the maximal pro-p extension of k which is unramified outside S and completely decomposed at T_0.

Then we have a canonical isomorphism

$$\phi_S^{T_0} : \mathop{\ast}_{\mathfrak{p}\in T_0(k_S^{T_0}(p))} G_{\mathfrak{p}}(k(p)|k) * \mathop{\ast}_{\mathfrak{p}\notin S(k_S^{T_0}(p))} T_{\mathfrak{p}}(k(p)|k) \xrightarrow{\sim} G(k(p)|k_S^{T_0}(p)).$$

Observe that T_0 may contain the set $S_p \cup S_\infty$ (and then the cyclotomic $\mathbb{Z}_p$-extension of k is not contained in $k_S^{T_0}(p)$). Furthermore we would like to mention that this result, in the case where S is the set of all places of k, is not an easy consequence of the theorem of Pop, although the proof of that theorem is much more difficult than this one which is only based on the theorem of Grunwald/Wang. From Pop's result it only follows that we have a free pro-p product decomposition into decomposition groups over the field k^{T_0} (the maximal Galois extension of k which is completely decomposed at all primes of T_0) whereas we show that this decomposition already exists over the maximal p-extension of k inside k^{T_0}.

Finally, I would like to thank Alexander Schmidt for many helpful discussions on this subject.

1 Free Products

We briefly collect some facts on free products of profinite groups. For a more detailed presentation and proofs we refer the reader to [4], chap. IV and chap. X §1 and [2].

A profinite space is a topological inverse limit of finite discrete spaces and a pro-$\mathfrak{c}$-group is a profinite group which is the inverse limit of groups in a full class of finite groups $\mathfrak{c}$ which is closed under taking subgroups, quotients and extensions.

Definition 1.1 *Let T be a profinite space. A bundle of pro-$\mathfrak{c}$-groups*

$$\mathcal{G} = (\mathcal{G}, pr, T)$$

over T is a group object in the category of profinite spaces over T together with a continuous structure map $pr : \mathcal{G} \to T$ such that the fibre $\mathcal{G}_t$ of $\mathcal{G}$ over every point $t \in T$ is a pro-$\mathfrak{c}$-group.

Example 1. If G is a pro-$\mathfrak{c}$-group and T a profinite space, then we always have the constant bundle $(G \times T, pr, T)$, where pr is the projection $G \times T \to T$.

Example 2. Let $\{G_t\}_{t\in T}$ be a continuous family of closed subgroups of a pro-$\mathfrak{c}$-group G indexed by the points of a profinite space T, i.e. it has the property that for every open subgroup $U \subseteq G$ the set $T(U) = \{t \in T \mid G_t \subseteq U\}$ is open in T. Then

$$\mathcal{G} = \{(g, t) \in G \times T \mid g \in G_t\}$$

is in a natural way a bundle of pro-$\mathfrak{c}$-groups over T.

Example 3. Let $\bar{T} = T \cup \{*\}$ be the one-point compactification of a discrete set T. Let $\{G_i\}_{i\in T}$ be a (discrete) family of pro-$\mathfrak{c}$-groups. Then the bundle $\mathcal{G}$ over $\bar{T}$ is defined by

$$\mathcal{G} := \dot{\bigcup_{i\in T}} G_i \,\dot{\cup}\, \{*\}\,,$$

with the following topology: $G_i \subseteq \mathcal{G}$ (together with its profinite topology) is open in $\mathcal{G}$ for all i, and for every open neighbourhood $V \subseteq \bar{T}$ of $* \in \bar{T}$, let

$$\dot{\bigcup_{\substack{i \in V \\ i \neq *}}} G_i \,\dot{\cup}\, \{*\}$$

be an open neighbourhood of $* \in \mathcal{G}$. One checks that the map

$$p : \mathcal{G} \to \bar{T};\; G_i \ni g_i \mapsto i,\; * \mapsto *$$

is continuous. Viewing $\{*\}$ as the group with one element, we see that the group operations on the G_i's induce the structure of a bundle of pro-$\mathfrak{c}$-groups on the triple $(\mathcal{G}, p, \bar{T})$.

Definition 1.2 *A morphism of bundles*

$$\phi : (\mathcal{G}, pr_{\mathcal{G}}, T) \to (\mathcal{H}, pr_{\mathcal{H}}, S)$$

is a pair $\phi_{\mathcal{G}} : \mathcal{G} \to \mathcal{H}$, $\phi_T : T \to S$ of continuous maps such that

(i) *the diagram*

$$\begin{tikzcd}
\mathcal{G} \arrow[r, "\phi_{\mathcal{G}}"] \arrow[d, "pr_{\mathcal{G}}"'] & \mathcal{H} \arrow[d, "pr_{\mathcal{H}}"] \\
T \arrow[r, "\phi_T"'] & S
\end{tikzcd}$$

commutes and

(ii) *for every $t \in T$ the associated map $\phi_t : \mathcal{G}_t \to \mathcal{H}_{\phi_T(t)}$ is a group homomorphism.*

We say that ϕ is surjective if $\phi_{\mathcal{G}}$ (and hence also ϕ_T) is surjective.

We will not distinguish between the pro-$\mathfrak{c}$-group G and the bundle $(G, pr, \{*\})$ over the one point space $\{*\}$. In particular, a morphism from a bundle $(\mathcal{G}, pr, T)$ to a group G is a continuous map $\phi : \mathcal{G} \to G$ such that the induced maps $\phi_t : \mathcal{G}_t \to G$ are group homomorphisms for every $t \in T$.

Definition 1.3 *The free pro-$\mathfrak{c}$-product of a bundle $(\mathcal{G}, pr, T)$ of pro-$\mathfrak{c}$-groups is a pro-$\mathfrak{c}$-group*

$$G = \mathop{\ast}_{T} \mathcal{G}$$

together with a morphism $\omega : \mathcal{G} \to G$, which has the following universal property: for every morphism $f : \mathcal{G} \to H$ from $\mathcal{G}$ to a pro-$\mathfrak{c}$-group H there exists a unique homomorphism of pro-$\mathfrak{c}$-groups $\phi : G \to H$ with $f = \phi \circ \omega$.

Proposition 1.4 *The free pro-$\mathfrak{c}$-product of the bundle $\mathcal{G}$ of pro-$\mathfrak{c}$-groups over T exists and is unique up to unique isomorphism.*

Let $\mathcal{G}$ be a bundle of pro-$\mathfrak{c}$-groups over a profinite space T and let $\{\mathcal{G}_t\}_{t\in T}$ be its fibers, i.e.

$$\mathcal{G} = \dot{\bigcup_{t\in T}} \mathcal{G}_t.$$

For the free pro-$\mathfrak{c}$-product of the bundle $(\mathcal{G}, pr, T)$ we often write

$$\mathop{\ast}_{T} \mathcal{G} = \mathop{\ast}_{t\in T} \mathcal{G}_t.$$

Proposition 1.5 *Let*

$$(\mathcal{G}, p, T) = \varprojlim_{i\in I} (\mathcal{G}_i, p_i, T_i)$$

be the inverse limit of the pro-$\mathfrak{c}$-group bundles $\mathcal{G}_i$. Then

$$\mathop{\ast}_{T} \mathcal{G} = \varprojlim_{i\in I} \mathop{\ast}_{T_i} \mathcal{G}_i.$$

Let G be a pro-$\mathfrak{c}$-group and let $\{G_t\}_{t\in T}$ be a continuous family of closed subgroups indexed by the points of a profinite space T, and so $\mathcal{G} = \{(g,t) \in G\times T \mid g\in G_t\}$ is a bundle over T. We have a canonical homomorphism

$$\phi : \mathop{\ast}_{T} \mathcal{G} \longrightarrow G.$$

Definition 1.6 *A pro-$\mathfrak{c}$-group G is the free product of the continuous family $\{G_t\}_{t\in T}$ if ϕ is an isomorphism.*

Now we consider the cohomology of a free product in the following case:

Let $T = \varprojlim_\lambda \bar{T}_\lambda$, where the sets $\bar{T}_\lambda = T_\lambda \cup \{*_\lambda\}$ are the one-point compactifications of discrete sets T_λ. Let $\mathcal{G} = \varprojlim_\lambda \mathcal{G}_\lambda$ be the projective limit of bundles $\mathcal{G}_\lambda = \dot{\bigcup}_{t_\lambda\in T_\lambda} G_{t_\lambda} \;\dot{\bigcup}\, \{*_\lambda\}$.

Let A be an abelian torsion group on which the groups $\ast_{\bar{T}_\lambda}\mathcal{G}_\lambda$ act and assume that these actions are compatible with respect to the transition maps. Then A is also a G-module where $G = \mathop{\ast}_{T}\mathcal{G}$.

Proposition 1.7 *With the notation and assumptions as above there is an exact sequence*

$$0\to A/A^G \to \varinjlim_{\lambda} \bigoplus_{T_\lambda} A/A^{G_{t_\lambda}} \to H^1(G,A) \to \varinjlim_{\lambda} \bigoplus_{T_\lambda} H^1(G_{t_\lambda},A)\to 0$$

and isomorphisms $$H^i(G,A) = \varinjlim_{\lambda} \bigoplus_{T_\lambda} H^i(G_{t_\lambda},A), \quad i\ge 2.$$

Proof: Using proposition 1.5, we have

$$H^i(G,A) = \varinjlim_{\lambda} H^i(\mathop{\ast}_{\bar{T}_\lambda}\mathcal{G}_\lambda, A), \quad i\ge 0,$$

and so the result follows from [4], theorem (4.1.4). $\square$

If k is a number field, then we denote the one-point compactification of the set of all places of k by $\mathrm{Sp}(k)$. The compactifying point will be denoted by η_k. For an infinite extension $K|k$, we set

$$\mathrm{Sp}(K) = \varprojlim_{k'} \mathrm{Sp}(k'),$$

where $k'|k$ runs through all finite subextensions of K. Let S be a set of primes of k and $\bar{S}$ its closure in $\mathrm{Sp}(k)$. The pre-image $\bar{S}(K)$ of $\bar{S}$ under the natural projection $\mathrm{Sp}(K) \to \mathrm{Sp}(k)$ is the closure of the set $S(K)$ of all prolongations of primes in S to K in $\mathrm{Sp}(K)$.

Let $M \supseteq K \supseteq k$ be (possibly infinite) extensions of k such that $M|K$ is a Galois extension and $G(M|K)$ is a pro-$\mathfrak{c}$-group. Let S be a set of primes of k. For a fixed section $s : \bar{S}(K) \to \bar{S}(M)$ of the natural projection $\bar{S}(M) \to \bar{S}(K)$ we consider the family $\{G_{s(\mathfrak{p})}(M|K)\}_{\mathfrak{p}\in\bar{S}(K)}$ of decomposition groups and the family $\{T_{s(\mathfrak{p})}(M|K)\}_{\mathfrak{p}\in\bar{S}(K)}$ of inertia groups, where by convention $G_{\eta_M} = \{1\}$. Since a finite extension of number fields is ramified only at finitely many primes, the later is a continuous family of subgroups of $G(M|K)$ indexed by $\bar{S}(K)$. We obtain a natural homomorphism

$$\varphi : \mathop{\ast}_{S(K)} T_{s(\mathfrak{p})}(M|K) \to G(M|K)$$

and, if $S(k)$ is finite, a homomorphism

$$\phi : \mathop{\ast}_{S(K)} G_{s(\mathfrak{p})}(M|K) \to G(M|K).$$

If $\mathfrak{c}$ is the class of p-groups, where p is a prime number, we have the following well-known

Lemma 1.8 *Let $f : G' \longrightarrow G$ be a homomorphism of pro-p-groups. Then f is an isomorphism if and only if the induced homomorphism*

$$H^i(f) : H^i(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^i(G', \mathbb{Z}/p\mathbb{Z})$$

is an isomorphism for $i = 1$ and injective for $i = 2$.

In particular, it follows that the questions whether the homomorphisms ϕ or φ are isomorphisms (in the case of pro-p-groups) do not depend on the section s. In the following we will omit the chosen section s in the notation.

For the cohomology of a free product with values in a torsion group A (considered as a module with trivial action) it follows from proposition 1.7 the

Proposition 1.9 *With the notation as above let S_1 and S_2 be sets of primes of k where S_1 is finite. Then, for $i \geq 1$, the following holds:*

$$H^i\big(\mathop{\ast}_{\mathfrak{p}\in S_1(K)} G_{\mathfrak{p}}(M|K) * \mathop{\ast}_{\mathfrak{p}\in S_2(K)} T_{\mathfrak{p}}(M|K), A\big)$$
$$= \varinjlim_{k'} \bigoplus_{\mathfrak{p}\in S_1(k')} H^i(G_{\mathfrak{p}}(M'|k'), A) \oplus \varinjlim_{k'} \bigoplus_{\mathfrak{p}\in S_2(k')} H^i(T_{\mathfrak{p}}(M'|k'), A).$$

where k' runs through all finite subextensions of k in K and M' is the maximal pro-$\mathfrak{c}$ Galois subextension of $M|k'$ (so $M = \varinjlim M'$).

The limits on the right-hand side depend on K and not on k and we denote them by

$$\sideset{}{'}\bigoplus_{\mathfrak{p}\in S_1(K)} H^i(G_{\mathfrak{p}}(M|K), A) \quad \text{and} \quad \sideset{}{'}\bigoplus_{\mathfrak{p}\in S_2(K)} H^i(T_{\mathfrak{p}}(M|K), A).$$

2 Galois Groups of large Number Fields

Let k be a number field and $\mathcal{P}$ the set of all primes of k. Let p be a prime number and $S \supseteq T$ sets of primes of k, where S contains the set $S_p \cup S_\infty$ of archimedean primes and primes above p, and let k_S be the maximal extension of k which is unramified outside S.

We denote the density of a set S of primes of k by $\delta(S)$ and the inertia subgroup of the decomposition group $G_\mathfrak{p}(k)$ by $T_\mathfrak{p}(k)$. In the following we write $H^i(-)$ for $H^i(-, \mathbb{Z}/p\mathbb{Z})$.

One version of the theorem of Grunwald/Wang says (see [4], theorem (9.2.2))

Theorem 2.1 *Let k be a number field and let $S \supseteq T$ be sets of primes of k, where $S \supseteq S_p \cup S_\infty$, $\delta(S) = 1$ and T is finite. Then the canonical homomorphism*

$$H^1(k_S|k) \longrightarrow \bigoplus_{\mathfrak{p}\in T} H^1(G_\mathfrak{p}(k))$$

is surjective.

Corollary 2.2 *Let k be a number field, and let T and T_0 be sets of primes such that T_0 is finite, $\delta(T) = 0$ and $T \cap T_0 = \varnothing$. Then the canonical homomorphism*

$$H^1(\bar{k}|k) \longrightarrow \bigoplus_{\mathfrak{p}\in T_0} H^1(G_\mathfrak{p}(k)) \oplus \bigoplus_{\mathfrak{p}\in T} H^1(T_\mathfrak{p}(k))^{G_\mathfrak{p}(k)}$$

is surjective.

Proof: Let $T_1 = T_0 \cup S_p \cup S_\infty$ and $S = (\mathcal{P}\backslash T) \cup S_p \cup S_\infty$. It follows that $\delta(S) = 1$, $\mathcal{P}\backslash S = T\backslash(S_p \cup S_\infty)$ and $T_1 \subset S$.

By theorem 2.1, the canonical map

$$H^1(k_S|k) \longrightarrow \bigoplus_{T_1} H^1(G_\mathfrak{p}(k))$$

is surjective. Furthermore, by [4] corollary (10.5.3), we have a canonical isomorphism

$$H^1(\bar{k}|k_S) \xrightarrow{\sim} \bigoplus_{\mathfrak{p}\notin S(k_S)}{}' \; H^1(T_\mathfrak{p}(k)),$$

and so an isomorphism

$$H^1(\bar{k}|k_S)^{G(k_S|k)} \xrightarrow{\sim} \bigoplus_{\mathfrak{p}\notin S(k)} H^1(T_\mathfrak{p}(k))^{G_\mathfrak{p}(k)}.$$

Consider the commutative and exact diagram

$$\begin{tikzcd}
H^1(\bar{k}|k_S)^{G(k_S|k)} \arrow[r, "\sim"] & \bigoplus_{T\backslash(S_p\cup S_\infty)} H^1(T_{\mathfrak{p}}(k))^{G_{\mathfrak{p}}(k)} \\
H^1(\bar{k}|k) \arrow[u] \arrow[r] & \bigoplus_{T_1} H^1(G_{\mathfrak{p}}(k)) \oplus \bigoplus_{T\backslash(S_p\cup S_\infty)} H^1(T_{\mathfrak{p}}(k))^{G_{\mathfrak{p}}(k)} \arrow[u, two heads] \\
H^1(k_S|k) \arrow[u, hook] \arrow[r, two heads] & \bigoplus_{T_1} H^1(G_{\mathfrak{p}}(k)) \arrow[u, hook]
\end{tikzcd}$$

We will show that the vertical upper map on the left-hand side is surjective. Using the Hochschild-Serre spectral sequence, we have to show that the inflation map

$$H^2(k_S|k) \longrightarrow H^2(\bar{k}|k)$$

is injective. But this follows from the commutative diagram

$$\begin{tikzcd}
H^2(\bar{k}|k) \arrow[r, hook] & \bigoplus_{\mathcal{P}} H^2(G_{\mathfrak{p}}(k)) \\
H^2(k_S|k) \arrow[u] \arrow[r, hook] & \bigoplus_{S} H^2(G_{\mathfrak{p}}(k)) \arrow[u, hook]
\end{tikzcd}$$

where the lower horizontal map is injective since $\delta(S) = 1$, see [4] theorem (9.1.8).

It follows that the map

$$H^1(\bar{k}|k) \longrightarrow \bigoplus_{T_1} H^1(G_{\mathfrak{p}}(k)) \ \oplus \bigoplus_{T\backslash(S_p\cup S_\infty)} H^1(T_{\mathfrak{p}}(k))^{G_{\mathfrak{p}}(k)}$$

is surjective. Since the maps $H^1(G_{\mathfrak{p}}(k)) \to H^1(T_{\mathfrak{p}}(k))^{G_{\mathfrak{p}}(k)}$ are surjective and the set T is contained in $(T_1\backslash T_0) \cup (T\backslash(S_p \cup S_\infty))$, the desired result follows. $\square$

For a number field k and sets S, T_0 of primes of k recall that

$k_S^{T_0}(p)$ is the maximal p-extension of k which is unramified outside S and completely decomposed at T_0.

For a prime $\mathfrak{p} \in S$ and a fixed extension $\mathfrak{P}$ of $\mathfrak{p}$ to a number field $K|k$ we denote the completion of K with respect to $\mathfrak{P}$ by $K_{\mathfrak{p}}$.

Proposition 2.3 *Let S, T_0 be sets of primes of k with $T_0 \cup S_p \cup S_\infty \subseteq S$ such that T_0 is finite and $\delta(S) = 1$. Then*

$$(k_S^{T_0}(p))_{\mathfrak{p}} = \begin{cases} k_{\mathfrak{p}}(p), & \textit{if } \mathfrak{p} \in S\backslash T_0, \\ k_{\mathfrak{p}}^{nr}(p), & \textit{if } \mathfrak{p} \notin S, \\ k_{\mathfrak{p}}, & \textit{if } \mathfrak{p} \in T_0. \end{cases}$$

Proof: Let $T = \mathcal{P}\backslash S$. For a prime $\mathfrak{p}_0$ of k let $\mathfrak{P}_0$ be a fixed extension to $k_S^{T_0}(p)$. Let $K|k$ be a finite Galois extension inside $k_S^{T_0}(p)$ and let $\overline{\mathfrak{P}}_0$ be the restriction of $\mathfrak{P}_0$ to K.

Let $\mathfrak{p}_0 \in S\backslash T_0$. By theorem 2.1, the canonical homomorphism

$$H^1(k_S|K) \longrightarrow H^1(G_{\overline{\mathfrak{P}}_0}(K)) \oplus \bigoplus_{T_0(K)} H^1(G_{\mathfrak{p}}(k))$$

is surjective. In particular, for every $\alpha_{\overline{\mathfrak{P}}_0} \in H^1(G_{\overline{\mathfrak{P}}_0}(K))$ there exists an element $\beta \in H^1(k_S|K)$ which is mapped to $(\alpha_{\overline{\mathfrak{P}}_0}, 0, \dots, 0)$. But β lies in the subgroup $H^1(k_S^{T_0}(p)|K)$ of $H^1(k_S|K)$. Therefore

$$H^1(k_S^{T_0}(p)|K) \longrightarrow H^1(G_{\overline{\mathfrak{P}}_0}(K))$$

is surjective, and so we proved the first assertion.

Now let $\mathfrak{p}_0 \in T$. Again by theorem 2.1, the canonical homomorphism

$$H^1(k_{S\cup\{\mathfrak{p}_0\}}|K) \longrightarrow H^1(G_{\overline{\mathfrak{P}}_0}(K)) \oplus \bigoplus_{T_0(K)} H^1(G_{\mathfrak{p}}(k))$$

is surjective. Therefore, for every

$$\alpha_{\overline{\mathfrak{P}}_0} \in H^1(G_{\overline{\mathfrak{P}}_0}(K)/T_{\overline{\mathfrak{P}}_0}(K)) \subseteq H^1(G_{\overline{\mathfrak{P}}_0}(K))$$

there exists $\beta \in H^1(k_{S\cup\{\mathfrak{p}_0\}}|K)$ which is mapped to $(\alpha_{\overline{\mathfrak{P}}_0}, 0, \dots, 0)$ and is therefore contained in $H^1(k_S^{T_0}(p)|K)$. Thus

$$H^1(k_S^{T_0}(p)|K) \longrightarrow H^1(G_{\overline{\mathfrak{P}}_0}(K)/T_{\overline{\mathfrak{P}}_0}(K))$$

is surjective. This proves the second assertion and the third is trivial. $\square$

Corollary 2.4 *Let k be a number field and let S, T_0 be sets of primes of k such that $T_0 \cup S_p \cup S_\infty \subseteq S$, $\delta(S) = 1$ and T_0 is finite. Then the canonical homomorphism*

$$H^1(k(p)|k_S^{T_0}(p)) \longrightarrow \sideset{}{'}\bigoplus_{\mathfrak{p}\in T_0(k_S^{T_0}(p))} H^1(G_{\mathfrak{p}}(k(p)|k)) \oplus \sideset{}{'}\bigoplus_{\mathfrak{p}\notin S(k_S^{T_0}(p))} H^1(T_{\mathfrak{p}}(k(p)|k))$$

is bijective and

$$H^2(k(p)|k_S^{T_0}(p)) \longrightarrow \sideset{}{'}\bigoplus_{\mathfrak{p}\in T_0(k_S^{T_0}(p))} H^2(G_{\mathfrak{p}}(k(p)|k))$$

is injective.

Proof: Using corollary 2.2 and taking the inductive limit over all finite subextensions of $k_S^{T_0}(p)|k$, we obtain a surjective homomorphism

$$H^1(\bar{k}|k_S^{T_0}(p)) \twoheadrightarrow \bigoplus_{\mathfrak{p}\in T_0(k_S^{T_0}(p))}{}' H^1(G_{\mathfrak{p}}(k)) \oplus \bigoplus_{\mathfrak{p}\notin S(k_S^{T_0}(p))}{}' H^1(T_{\mathfrak{p}}(k))^{G_{\mathfrak{p}}(k_S^{T_0}(p))}.$$

By proposition 2.3, we have

$$G_{\mathfrak{p}}(k(p)|k_S^{T_0}(p)) = T_{\mathfrak{p}}(k(p)|k) \quad \text{for } \mathfrak{p} \notin S,$$

and so we obtain a surjection

$$H^1(k(p)|k_S^{T_0}(p)) \twoheadrightarrow \bigoplus_{\mathfrak{p}\in T_0(k_S^{T_0}(p))}{}' H^1(G_{\mathfrak{p}}(k(p)|k)) \oplus \bigoplus_{\mathfrak{p}\notin S(k_S^{T_0}(p))}{}' H^1(T_{\mathfrak{p}}(k(p)|k)).$$

Since the groups $G_{\mathfrak{p}}(k(p)|k)$ for $\mathfrak{p} \in T_0$ and $T_{\mathfrak{p}}(k(p)|k)$ for $\mathfrak{p} \notin S$ generate the group $G(k(p)|k_S^{T_0}(p))$, the map above is injective. Thus we proved the first assertion.

By [4] theorem (9.1.8), we have an injection

$$H^2(\bar{k}|k_S^{T_0}(p)) \hookrightarrow \bigoplus_{\mathfrak{p}\in T_0(k_S^{T_0}(p))}{}' H^2(G_{\mathfrak{p}}(k)) \oplus \bigoplus_{\mathfrak{p}\notin T_0(k_S^{T_0}(p))}{}' H^2(G_{\mathfrak{p}}(k_S^{T_0}(p))).$$

Since $H^2(\bar{k}|K) = H^2(k(p)|K)$ and $H^2(G_{\mathfrak{p}}(K)) = H^2(G_{\mathfrak{p}}(k(p)|K))$, see [4] theorem (10.4.8) and theorem (7.5.7), we get an injection

$$H^2(k(p)|k_S^{T_0}(p)) \hookrightarrow \bigoplus_{\mathfrak{p}\in T_0(k_S^{T_0}(p))}{}' H^2(G_{\mathfrak{p}}(k(p)|k)) \oplus \bigoplus_{\mathfrak{p}\notin T_0(k_S^{T_0}(p))}{}' H^2(G_{\mathfrak{p}}(k(p)|k_S^{T_0}(p))).$$

From proposition 2.3 it follows that

$$H^2(G_{\mathfrak{p}}(k(p)|k_S^{T_0}(p))) = 0 \quad \text{for } \mathfrak{p} \notin T_0,$$

since $G_{\mathfrak{p}}(k(p)|k_S^{T_0}(p)) = 1$ for $\mathfrak{p} \in S \backslash T_0$ and $cd_p\, G_{\mathfrak{p}}(k(p)|k_S^{T_0}(p)) \leq 1$ for $\mathfrak{p} \notin S$. This proves the second assertion. □

Using lemma 1.8 and corollary 2.4, we obtain the following theorem.

Theorem 2.5 *Let k be a number field and let S, T_0 be sets of primes of k such that $\delta(S) = 1$, $S_p \cup S_\infty \subset S$ and T_0 is a finite subset of S. Then there is a canonical isomorphism*

$$\phi_S^{T_0} : \mathop{\ast}_{\mathfrak{p}\in T_0(k_S^{T_0}(p))} G_{\mathfrak{p}}(k(p)|k) * \mathop{\ast}_{\mathfrak{p}\notin S(k_S^{T_0}(p))} T_{\mathfrak{p}}(k(p)|k) \xrightarrow{\sim} G(k(p)|k_S^{T_0}(p)).$$

In particular, if $S = \mathcal{P}$, then

$$\mathop{\ast}_{\mathfrak{p}\in T_0(k^{T_0}(p))} G_{\mathfrak{p}}(k(p)|k) \xrightarrow{\sim} G(k(p)|k^{T_0}(p)).$$

References

[1] Fried, M.D., Haran, D., Völklein, H. *Absolute Galois group of the totally real numbers.* C.R. Acad. Sci., Paris **317** (1993) 995-999

[2] Neukirch, J. *Freie Produkte pro-endlicher Gruppen und ihre Kohomologie.* Archiv der Math. **22** (1971) 337–357

[3] Neukirch, J. *Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen.* J. für reine u. angew. Math. **259** (1973) 1-47

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

[5] Pop, F. *Embedding problems over large fields.* Ann. of Math. **144** (1996) 1-34

[6] Schmidt, A. *On the relation between* 2 *and* ∞ *in Galois cohomology of number fields.* Comp. Math. **133** (2002) 267-288