

On generators of the group $\widehat{H}^{-1}(\text{Gal}(L/K), E_L)$ in some abelian p -extension L/K

Emmanuel HALLOUIN and Marc PERRET*

September 25, 2007

À Gille Lachaud, en l'honneur de ses soixante ans.

Introduction

The main motivation of this work is Shafarevich theorem on class fields towers, as in the spirit of [Ser94], Chap I, §4.4. Let L/K be a unramified (here, unramifiedness refers also to the infinite primes throughout) Galois extension of number fields whose Galois group G is a finite p -group (p a prime integer). We know that:

$$d_p H^3(G, \mathbb{Z}) = d_p H^2(G, \mathbb{Z}/p\mathbb{Z}) - d_p H^1(G, \mathbb{Z}/p\mathbb{Z}).$$

where $d_p \mathcal{G}$ denotes the p -rank of a finite p -group \mathcal{G} . If moreover the class number of L is not divisible by p then:

$$d_p H^3(G, \mathbb{Z}) \leq r_1 + r_2 \tag{1}$$

where (r_1, r_2) is the signature of the number field K . Briefly, the proof works as follows. Let C_L be the idèle class group of L and E_L its unit group, then:

$$\forall q \in \mathbb{Z}, \quad \widehat{H}^q(G, C_L) \simeq \widehat{H}^{q+1}(G, E_L) \quad \text{and} \quad \widehat{H}^q(G, C_L) \simeq \widehat{H}^{q-2}(G, \mathbb{Z}).$$

The first isomorphism follows from the fact that L has a class number not divisible by p while the second one is part of class field theory. Thus:

$$\widehat{H}^{q+1}(G, E_L) \simeq \widehat{H}^{q-2}(G, \mathbb{Z}). \tag{2}$$

The inequality (1) comes from the specialization at $q = -1$ of this isomorphism since the rank of $\widehat{H}^0(G, E_L) = E_K/N_{L/K}(E_L)$ is easily bounded thanks to Dirichlet's unit theorem.

Together with Golod-Shafarevich inequality, which states that $d_p H^2(G, \mathbb{Z}/p\mathbb{Z}) > (d_p H^1(G, \mathbb{Z}/p\mathbb{Z}))^2/4$, inequality (1) implies that:

$$\frac{(d_p H^1(G, \mathbb{Z}/p\mathbb{Z}))^2}{4} - d_p H^1(G, \mathbb{Z}/p\mathbb{Z}) < r_1 + r_2.$$

A famous consequence is the following: if a number field K satisfies the quadratic (in $d_p \text{Cl}(K)$) inequality:

$$(d_p \text{Cl}(K))^2/4 - d_p \text{Cl}(K) \geq r_1 + r_2,$$

then its p -class field tower is infinite.

A cubic (in $d_p \text{Cl}(K)$) infiniteness criterion of the p -class field tower over a field k already exists (see [NSW00], proof of corollary 10.8.11, chapter 10). Unfortunately, it works only if there is an action of $\text{Gal}(k/k_0)$ for a quadratic subfield k_0 of k . In order to find an unconditional cubic analogue of this criterion, one can specialize the isomorphism (2) at $q = -2$. This yields the following equality:

$$d_p \widehat{H}^{-1}(G, E_L) = d_p H^3(G, \mathbb{Z}/p\mathbb{Z}) - d_p H^2(G, \mathbb{Z}/p\mathbb{Z}) + d_p H^1(G, \mathbb{Z}/p\mathbb{Z}).$$

hence, it is crucial as a first step to find an upper bound for the p -rank $d_p \widehat{H}^{-1}(G, E_L)$ when $\text{Cl}(L)$ is trivial. In this paper, we prove results about generators of this group in some special cases. More precisely, we compute the p -rank and exhibit an explicit basis of $\widehat{H}^{-1}(G, E_L)$ when L/K is an unramified abelian p -extension whose Galois group has exactly two generators..

*Laboratoire Emile Picard, Institut de Mathématiques de Toulouse, France.

Notations — Let K be a number field. We denote by Σ_K the set of its finite places, $\text{Div}(K)$ its ideal group and $\text{Cl}(K)$ its ideal class group. To each finite place $v \in \Sigma_K$ one can associate a unique prime ideal \mathfrak{p}_v of K and to each $x \in K^*$, there corresponds a principal ideal $\langle x \rangle_K$ of K .

If L/K is a Galois extension of number fields, then for each $v \in \Sigma_K$, $\Sigma_{L,v}$ denotes the subset of places $w \in \Sigma_L$ above v (for short $w \mid v$) and f_v the residual degree of any $w \in \Sigma_{L,v}$ over K . The map $j_{L/K} : \text{Div}(K) \rightarrow \text{Div}(L)$ is the usual extension of ideals.

Let G be a finite group and M be a multiplicative G -module. The norm map $N_G : M \rightarrow M$ is defined by $x \mapsto \prod_{g \in G} g(x)$; its kernel is denoted by $M[N_G]$. The augmentation ideal $I_G M = \left\langle \frac{g(x)}{x}, x \in M, g \in G \right\rangle$ is of importance. Of course, one has $I_G M \subset M[N_G]$; the quotient of these two subgroups is nothing else than the Tate cohomology group:

$$\widehat{H}^{-1}(G, M) \stackrel{\text{def.}}{=} \frac{M[N_G]}{I_G M}$$

in which we are interested (see [Ser68] for an introduction to the negative cohomology groups). For $u \in M[N_G]$, we denote by $[u]$ the class of u in $\widehat{H}^{-1}(G, M)$.

1 The cyclic case

Let L/K be a cyclic extension with Galois group $G = \langle g \rangle$. A classical consequence of Hilbert 90 theorem states that the kernel of the norm N_G equals the augmentation ideal: $L^*[N_G] = I_G L^*$. In cohomological terms, this means that:

$$H^1(G, L^*) = \{1\} \quad \implies \quad \widehat{H}^{-1}(G, L^*) = \{1\}.$$

Another easy consequence already known is that:

Proposition 1 *Let L/K be an unramified cyclic extension with Galois group $G = \langle g \rangle$. Then the map:*

$$\varphi_g : \begin{array}{ccc} \text{Ker}(\text{Cl}(K) \rightarrow \text{Cl}(L)) & \longrightarrow & \widehat{H}^{-1}(G, E_L) \\ [I] & \longmapsto & \left[\frac{g(y)}{y} \right] \end{array},$$

is a group isomorphism, where $[I]$ denotes the ideal class of I and y is any generator of the extension of I to L .

Proof — The only non-trivial assertion is the surjectivity of the map. Let $u \in E_L[N_G]$, then there exists $y \in L^*$ such that $u = \frac{g(y)}{y}$. Thus the ideal $\langle y \rangle_L$ is fixed by the action of G . The extension L/K being unramified, the ideal $\langle y \rangle_L$ is the extension to L of some ideal I of K : $j_{L/K}(I) = \langle y \rangle_L$. Then $[u] = \varphi_g([I])$. \square

This proposition implies the following corollary:

Corollary 2 *Let K be a number field whose ideal class group is a cyclic p -group and L be its Hilbert class field. Suppose that L has class number one. Then for any generator g of $\text{Gal}(L/K)$ and any generator π of a prime ideal of L whose Frobenius equal to g , $\widehat{H}^{-1}(G, E_L)$ is a cyclic p -group generated by the class of $\sigma(\pi)/\pi$:*

$$\widehat{H}^{-1}(G, E_L) = \left\langle \left[\frac{g(\pi)}{\pi} \right] \right\rangle.$$

2 Some experiments with magma

With the help of `magma` and `pari/gp`, we have made some experiments and collect datas about the 2-rank of the group $\widehat{H}^{-1}(G, E_{K^i})$ in unramified finite 2-extensions K^i/K ($i = 1, 2$). In each case, we start with a quadratic complex number field K whose class group is a 2-group; tables of such fields can be found in [Lem]. We compute $K^1 = K^{\text{hilb}}$ and the group structure of $\widehat{H}^{-1}(E_{K^1}) \stackrel{\text{def.}}{=} \widehat{H}^{-1}(\text{Gal}(K^1/K), E_{K^1})$. If $\text{Cl}(K^1)$ is not trivial, we try to go further. We compute $K^2 = (K^1)^{\text{hilb}}$ and the group structure of $\widehat{H}^{-1}(E_{K^2}) \stackrel{\text{def.}}{=} \widehat{H}^{-1}(\text{Gal}(K^2/K), E_{K^2})$.

Here is the `magma` program we used:

```

clear ;
Q := RationalField() ;
dis := -84 ;
K<x> := QuadraticField(dis) ;

"Computation of K^hilb..." ;
Khilb := AbsoluteField(HilbertClassField(K)) ;
Khilb<y> := OptimizedRepresentation(Khilb) ;

"... computation of the unit group of K^hilb..." ;
E_Khilb, e_Khilb := UnitGroup(Khilb) ;

Gal_Khilb_Q, Aut_Khilb_Q, i := AutomorphismGroup(Khilb) ;
G := FixedGroup(Khilb, K) ;
Norm_G := map < Khilb -> Khilb | y :-> &* [i(g)(y) : g in G] > ;
N := hom < E_Khilb -> E_Khilb | [(e_Khilb * Norm_G * Inverse(e_Khilb))(E_Khilb.i) :
                                i in [1..NumberOfGenerators(E_Khilb)]] > ;

Ker_N := Kernel(N) ;
I_G := [i(g)(u)/u : u in Generators(E_Khilb) @ e_Khilb, g in G] ;
I_G := sub < E_Khilb | I_G @@ e_Khilb > ;
assert(I_G subset Ker_N) ;
printf "... structure of H^(-1)(G, E_M) = %o\n", Ker_N / I_G ;

```

Unfortunately, because of the difficulty of computing the unit group of a number field, only few computations achieved. In the following table, the notation $2 \cdot 4$ means that the group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

$\text{dis}(K)$	$\text{Cl}(K)$	$\text{Cl}(K^1)$	$\widehat{H}^{-1}(E_{K^1})$	$\text{Cl}(K^2)$	$\widehat{H}^{-1}(E_{K^2})$
-84	$2 \cdot 2$	1	$2 \cdot 2 \cdot 2$		
-120	$2 \cdot 2$	2	4	1	8
-260	$2 \cdot 4$	2	$2 \cdot 4$	1	$2 \cdot 8$
-280	$2 \cdot 2$	4	4	1	16
-308	$2 \cdot 4$	1	$2 \cdot 2 \cdot 4$		
-399	$2 \cdot 8$	1	$2 \cdot 2 \cdot 8$		
-408	$2 \cdot 2$	2	$2 \cdot 2 \cdot 2$	1	$2 \cdot 2 \cdot 4$
-420	$2 \cdot 2 \cdot 2$	$2 \cdot 2$	$2 \cdot 2 \cdot 2 \cdot 4$	1	unkown
-456	$2 \cdot 4$	1	$2 \cdot 2 \cdot 4$		

In the following section, we will explain why $d_2 \widehat{H}^{-1}(E_{K^1}) = 3$ when $d_2 \text{Cl}(K) = 2$ and $d_2 \text{Cl}(K^1) = 1$. In all the remaining known cases, we point out that $d_2 \widehat{H}^{-1}(E_{K^1}) = d_2 \widehat{H}^{-1}(E_{K^2})$.

3 When the Galois group has two generators

The goal of this section is to extend the results of §1 to the case of extensions whose Galois group is an abelian group generated by two elements.

First, we need to investigate the cohomology group with values in M^* . We still have:

Theorem 3 *Let K be a number field and M/K be an unramified abelian extension whose Galois group G is a p -group generated by two elements. Then $\widehat{H}^{-1}(G, M^*) = 1$.*

Proof — Since M/K is an unramified abelian extension, there exists a subgroup G' of $\text{Cl}(K)$ such that $G \simeq \text{Cl}(K)/G'$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be primes of K whose classes generate G' . If $G \simeq \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/p^\beta\mathbb{Z}$ with $\alpha \leq \beta$, we complete these primes by choosing $\mathfrak{p}, \mathfrak{q}$ primes of K such that their decomposition groups in M/K satisfy $D(\mathfrak{p}) = \langle (1, 1) \rangle$ and $D(\mathfrak{q}) = \langle (0, 1) \rangle$. Adjoining $\mathfrak{p}, \mathfrak{q}$ to the \mathfrak{p}_i 's leads to a system of generators of $\text{Cl}(K)$.

Let $H = \langle (1, 0) \rangle$. Then H and G/H are cyclic and, by construction, the decomposition groups in M/K satisfy:

$$\forall 1 \leq i \leq r, \quad D(\mathfrak{p}_i) \cap H = \{\text{id}\}, \quad D(\mathfrak{p}) \cap H = \{\text{id}\}, \quad D(\mathfrak{q}) \cap H = \{\text{id}\}.$$

Theorem 3 is implied by the two following lemmas. □

Lemma 4 *Let H be a normal cyclic subgroup of G . Then:*

$$\widehat{H}^{-1}(G, M^*) = \{1\} \iff \widehat{H}^{-1}(G/H, N_H(M^*)) = \{1\}.$$

Proof — Suppose that $\widehat{H}^{-1}(G, M^*) = \{1\}$. If $y \in N_H(M^*)[N_{G/H}]$, then there exists $z \in M^*$ such that $y = N_H(z)$ and $N_G(z) = N_{G/H}(N_H(z)) = N_{G/H}(y) = 1$. Thus, by hypothesis, $z \in M^*[N_G] = I_G M^*$:

$$\exists z_i \in M, g_i \in G, \quad z = \frac{g_1(z_1)}{z_1} \times \cdots \times \frac{g_r(z_r)}{z_r}.$$

Hence:

$$y = N_H(z) = \frac{g_1(N_H(z_1))}{N_H(z_1)} \times \cdots \times \frac{g_r(N_H(z_r))}{N_H(z_r)}.$$

Therefore $y \in I_{G/H} N_H(M^*)$.

Conversely, suppose that $\widehat{H}^{-1}(G/H, N_H(M^*)) = \{1\}$. If $z \in M^*[N_G]$ then $1 = N_G(z) = N_{G/H}(N_H(z))$ and thus $N_H(z) \in N_H(M^*)[N_{G/H}]$. By hypothesis, there exist $z_1, \dots, z_r \in M^*$ and $g_1, \dots, g_r \in G$ such that:

$$N_H(z) = \frac{g_1(N_H(z_1))}{N_H(z_1)} \times \cdots \times \frac{g_r(N_H(z_r))}{N_H(z_r)} = N_H \left(\frac{g_1(z_1)}{z_1} \times \cdots \times \frac{g_r(z_r)}{z_r} \right).$$

It follows that:

$$z \in I_G M^* \times M^*[N_H] = I_G M^* \times I_H M^* = I_G M^*,$$

because, H being cyclic, one has $M^*[N_H] = I_H M^*$. □

Lemma 5 *Let H be a cyclic subgroup of G such that G/H is also cyclic. If $\text{Cl}(K)$ can be generated by primes whose decomposition groups intersect H trivially, then $\widehat{H}^{-1}(G/H, N_H(M^*)) = \{1\}$.*

Proof — Let h be a generator of H and $g \in G$ such that $G = \langle g, h \rangle$. Let $L = M^H$ so that $\text{Gal}(L/K) = \langle g \rangle$.

Let $y \in N_H(M^*)[N_{G/H}]$. Since G/H is cyclic generated by g , there exists $b \in L$ such that $y = \frac{g(b)}{b}$.

Since $y \in N_H(M^*)$, it is a norm everywhere locally:

$$\begin{aligned} \forall w \in \Sigma_L, w(y) \equiv 0 \pmod{f_w} &\implies \forall w \in \Sigma_L, w \circ g(b) \equiv w(b) \pmod{f_w} \\ &\implies \forall v \in \Sigma_K, \forall w, w' \in \Sigma_{L,v}, w'(b) \equiv w(b) \pmod{f_w}. \end{aligned}$$

Note that there is no condition at infinity since infinite places are unramified by assumption. The last assertion implies that the ideal J of L defined by:

$$J = \prod_{w \in \Sigma_L} \mathfrak{p}_w^{-w(b) \bmod f_w} \quad (\text{for } x \in \mathbb{Z}, \text{ we choose } x \bmod f_w \in [0..f_w - 1]),$$

is the extension to L of the ideal I of K defined by:

$$I = \prod_{v \in \Sigma_K} \mathfrak{p}_v^{-w(b) \bmod f_w} \quad (\text{for each } v \in \Sigma_K, \text{ we choose } w \text{ a place of } \Sigma_{L,v}).$$

By hypothesis, $\text{Cl}(K)$ can be generated by prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of K whose decomposition groups satisfy $D(\mathfrak{p}_i) \cap H = \{\text{id}\}$. This means that all primes of L above each \mathfrak{p}_i split totally in M . There exists $a \in K$ and $e_1, \dots, e_r \in \mathbb{N}$ such that $\langle a \rangle = I \times \prod_i \mathfrak{p}_i^{e_i}$. By construction, the ideal ab of L has support on primes of L which split totally in M .

Now, recall that the local-global principle holds for norm equations in cyclic extensions. Thus, we deduce that $ab \in N_H(M^*)$. Finally, because $a \in K$, we have:

$$y = \frac{g(b)}{b} = \frac{g(ab)}{ab} \in I_{G/H} N_H(M^*),$$

which was to be proved. □

As in the cyclic case, the triviality of the -1 cohomological group with values in M^* implies something on the -1 cohomological group with values in E_M . To begin with, let us state the following easy proposition:

Proposition 6 *Let K be a number field and M/K be an unramified abelian extension with Galois group G a p -group of p -rank d . If M is principal, then $d_p \widehat{H}^{-1}(G, E_M) = \frac{d(d^2+5)}{6}$.*

Proof — In [Ser94] §4.4, thanks to class field theory, it is proved that:

$$\forall q \in \mathbb{Z}, \widehat{H}^{q+1}(G, E_M) \simeq \widehat{H}^{q-2}(G, \mathbb{Z}).$$

Hence, for $q = -2$, we obtain:

$$\widehat{H}^{-1}(G, E_M) \simeq \widehat{H}^{-4}(G, \mathbb{Z}).$$

By duality, it is enough to compute the p -rank of $H^4(G, \mathbb{Z})$. To this end, we start with the exact sequence of G -modules (trivial action) $0 \rightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0$ and we consider the long cohomology exact sequence:

$$\begin{aligned} 0 \rightarrow H^1(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^2(G, \mathbb{Z}) \xrightarrow{p} H^2(G, \mathbb{Z}) \rightarrow H^2(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow \\ H^3(G, \mathbb{Z}) \xrightarrow{p} H^3(G, \mathbb{Z}) \rightarrow H^3(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^4(G, \mathbb{Z})[p] \rightarrow 0. \end{aligned}$$

The logarithm of the product of the orders of these groups equals 0, therefore:

$$d_p H^4(G, \mathbb{Z}) = d_p H^3(G, \mathbb{Z}/p\mathbb{Z}) - d_p H^2(G, \mathbb{Z}/p\mathbb{Z}) + d_p H^1(G, \mathbb{Z}/p\mathbb{Z})$$

(recall that in a finite abelian p -group A , one has: $\#A[p] = p^{d_p A}$). It is now easy to conclude because:

$$d_p H^2(G, \mathbb{Z}/p\mathbb{Z}) = \frac{d(d+1)}{2} \quad \text{and} \quad d_p H^3(G, \mathbb{Z}/p\mathbb{Z}) = \frac{d(d+1)(d+2)}{6}$$

as it can be proved using Künneth's formula (see [NSW00], exercice 7, page 96). \square

Remark – The isomorphism of the beginning of this proof for $q = -1$ is a key step in the proof of Golod-Shafarevich's theorem.

Let us return to the case where $d_p(G) = 2$. Then, due to proposition 6, one has $d_p(G, E_M) = 3$. As in corollary 2, one can be more precise and exhibit a basis of $\widehat{H}^{-1}(G, E_M)$.

Proposition 7 *Let K be a number field and M/K an unramified abelian extension with Galois group G . If M has class number one and if $\widehat{H}^{-1}(G, M^*) = \{1\}$ then:*

$$\widehat{H}^{-1}(G, E_M) = \left\langle \left[\frac{\sigma_\pi(\pi)}{\pi} \right], \pi \text{ a prime element of } M \right\rangle.$$

where σ_π denotes the Frobenius at π .

Proof — Let π be a prime element of M and $g, g' \in G$ such that $g \equiv g' \pmod{D(\pi)}$, where $D(\pi)$ denotes the decomposition group of the ideal $\langle \pi \rangle_M$. Then there exists $\alpha \in \mathbb{N}$ such that $g^{-1}g' = \sigma_\pi^\alpha$ and thus:

$$\frac{g'(\pi)}{g(\pi)} = g \left(\frac{g^{-1}g'(\pi)}{\pi} \right) = g \left(\frac{\sigma_\pi^\alpha(\pi)}{\pi} \right) \equiv \frac{\sigma_\pi^\alpha(\pi)}{\pi} \equiv \left(\frac{\sigma_\pi(\pi)}{\pi} \right)^\alpha \pmod{I_G E_M}.$$

For every $v \in \Sigma_K$, we choose a generator π_v of one of the primes of M above \mathfrak{p}_v . We fix a section $\sigma \mapsto \tilde{\sigma}$ of the cononical projection map $G \rightarrow G/D(\pi_v)$. The elements $\tilde{\sigma}(\pi_v)$, when v runs in Σ_K and $\sigma \in G/D(v)$, describe a system of prime elements of M . Then every $z \in M$ factorizes into:

$$z = u \prod_{v \in \Sigma_K} \left(\prod_{\sigma \in G/D(v)} \tilde{\sigma}(\pi_v)^{e_{v,\sigma}} \right) \implies g(z) = g(u) \prod_{v \in \Sigma_K} \left(\prod_{\sigma \in G/D(v)} g\tilde{\sigma}(\pi_v)^{e_{v,\sigma}} \right)$$

for every $g \in G$. Of course $g\tilde{\sigma} \equiv \tilde{g\sigma} \pmod{D(\pi_v)}$, therefore there exists $\alpha_{v,\sigma} \in \mathbb{N}$ such that:

$$\begin{aligned} g\tilde{\sigma}(\pi_v) &= \left(\frac{\sigma_v(\pi_v)}{\pi_v} \right)^{\alpha_{v,\sigma}} \tilde{g\sigma}(\pi_v) \\ \implies g(z) &\in \langle g(u) \left\langle \frac{\sigma_\pi(\pi)}{\pi}, \pi \text{ a prime element of } M \right\rangle \tilde{\sigma}(\pi_v), v \in \Sigma_K, \sigma \in G/D(v) \rangle. \end{aligned}$$

Now start with $u \in E_M[N_G]$. By hypothesis, we know that $\widehat{H}^{-1}(G, M^*) = \{1\}$, i.e. $M^*[N_G] = I_G M^*$. Hence, if $G = \langle g_1, \dots, g_r \rangle$, there exists $z_1, \dots, z_r \in M^*$ such that $u = \frac{g_1(z_1)}{z_1} \dots \frac{g_r(z_r)}{z_r}$. Factorizing z_1, \dots, z_r into primes of M of the form $\tilde{\sigma}(\pi_v)$, one shows that:

$$u \in I_G E_M \left\langle \frac{\sigma_\pi(\pi)}{\pi}, \pi \text{ a prime element of } M \right\rangle \tilde{\sigma}(\pi_v), v \in \Sigma_K, \sigma \in G/D(v);$$

But, in this decomposition, since u is invertible, the element in the third group must be equal to 1. \square

Theorem 8 *Let K be a number field whose ideal class group is a p -group of rank two and M/K its Hilbert class field. Suppose that M has class number one. Then for any generators g_1, g_2 of $\text{Gal}(M/K)$ and any generators π_1, π_2, π_{12} of prime ideals of M with Frobenius equal to g_1, g_2 and g_1g_2 respectively, $\widehat{H}^{-1}(G, E_M)$ is generated by the classes of $g_1(\pi_1)/\pi_1, g_1(\pi_2)/\pi_2$ and $g_1g_2(\pi_{12})/\pi_{12}$:*

$$\widehat{H}^{-1}(G, E_M) = \left\langle \left[\frac{g_1(\pi_1)}{\pi_1} \right], \left[\frac{g_2(\pi_2)}{\pi_2} \right], \left[\frac{g_1g_2(\pi_{12})}{\pi_{12}} \right] \right\rangle.$$

Proof — For any prime element π of M , we denote its Frobenius by σ_π . By theorem 3, we have $\widehat{H}^{-1}(G, M^*) = \{1\}$ and thanks to the preceding result the group $\widehat{H}^{-1}(G, E_M)$ is generated by the classes of the elements $\frac{\sigma_\pi(\pi)}{\pi}$. Therefore, we only have to prove that the class modulo $I_G E_M$ of the element $u = \frac{\sigma_\pi(\pi)}{\pi}$ is contained in the subgroup generated by the $\frac{g_i(\pi_i)}{\pi_i}$ for $i = 1, 2, 12$.

To this end, put $H = \langle g_{12} \rangle$, $L = M^H$ and $\mathfrak{p} = \langle \pi \rangle_M \cap K$, $\mathfrak{p}_1 = \langle \pi_1 \rangle_M \cap K$, $\mathfrak{p}_2 = \langle \pi_2 \rangle_M \cap K$.

There exists $\alpha_1, \alpha_2 \in \mathbb{N}$ such that $\sigma_\pi = g_1^{\alpha_1} g_2^{\alpha_2}$ and, by Artin map, $\mathfrak{p} = a \mathfrak{p}_1^{\alpha_1} \mathfrak{p}_2^{\alpha_2}$ with $a \in K^*$. Since $\langle \sigma_i \rangle \cap H = \{\text{Id}\}$ for $i = 1, 2$, the primes \mathfrak{p}_i , $i = 1, 2$, totally split between L and M . Thus:

$$\begin{cases} j_{L/K}(\mathfrak{p}) = \langle N_H(\pi) \rangle_L \\ j_{L/K}(\mathfrak{p}_i) = \langle N_H(\pi_i) \rangle_L, i = 1, 2 \end{cases} \implies N_H(\pi) = av N_H(\pi_1)^{\alpha_1} N_H(\pi_2)^{\alpha_2},$$

where $v \in E_L$. Hence:

$$N_H(u) = N_H \left(\frac{\sigma_\pi(\pi)}{\pi} \right) = \frac{\sigma_\pi(N_H(\pi))}{N_H(\pi)} = \frac{\sigma_\pi(a)}{a} \frac{\sigma_\pi(v)}{v} N_H \left(\frac{\sigma_\pi(\pi_1)}{\pi_1} \right)^{\alpha_1} N_H \left(\frac{\sigma_\pi(\pi_2)}{\pi_2} \right)^{\alpha_2}.$$

Let us study the four terms in the right hand product. The first one is equal to 1 because $a \in K$. Since local-global principal occurs in cyclic extensions and since M/L is unramified, there exists $w \in E_M$ such that $v = N_H(w)$. Thus the second term $\frac{\sigma_\pi(v)}{v}$ equals $N_H \left(\frac{\sigma_\pi(w)}{w} \right)$. The third and fourth terms go in the same way: since g_1, g_2 generate G , the elements g_1 and g_1g_2 also generate G and there exists $\beta_1, \beta_2 \in \mathbb{N}$ such that $\sigma_\pi = g_1^{\beta_1} (g_1g_2)^{\beta_2}$. It follows that:

$$N_H \left(\frac{\sigma_\pi(\pi_1)}{\pi_1} \right) = N_H \left(\frac{g_1^{\beta_1}(\pi_1)}{\pi_1} \right) = N_H \left(\frac{g_1(w_1)}{w_1} \left(\frac{g_1(\pi_1)}{\pi_1} \right)^{\beta_1} \right)$$

where $w_1 \in E_M$.

In conclusion, u satisfies:

$$\begin{aligned} N_H(u) &= N_H \left(\frac{\sigma_\pi(w)}{w} \frac{g_1(w_1)}{w_1}^{\alpha_1} \frac{g_2(w_2)}{w_2}^{\alpha_1} \left(\frac{g_1(\pi_1)}{\pi_1} \right)^{\alpha_1 \beta_1} \left(\frac{g_2(\pi_2)}{\pi_2} \right)^{\alpha_2 \beta_2} \right) \\ &\implies u \times \left(\frac{\sigma_\pi(w)}{w} \frac{g_1(w_1)}{w_1}^{\alpha_1} \frac{g_2(w_2)}{w_2}^{\alpha_2} \left(\frac{g_1(\pi_1)}{\pi_1} \right)^{\alpha_1 \beta_1} \left(\frac{g_2(\pi_2)}{\pi_2} \right)^{\alpha_2 \beta_2} \right)^{-1} \in E_M[N_H]. \end{aligned}$$

Finally, due to the cyclic case, we know that $E_M[N_H] = I_H E_M \left\langle \frac{g_1g_2(\pi_{12})}{\pi_{12}} \right\rangle$ and thus:

$$u \text{ mod } I_G E_M \in \left\langle \frac{g_1(\pi_1)}{\pi_1}, \frac{g_2(\pi_2)}{\pi_2}, \frac{g_1g_2(\pi_{12})}{\pi_{12}} \right\rangle,$$

which was to be proved. □

Remark – All these results hold in the function field case for S -units where S is any non-empty finite set of places.

References

- [Lem] Franz Lemmermeyer. A survey on class field towers. <http://www.rzuser.uni.heidelberg.de/~hb3/cft.html>.
- [NSW00] Jurgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*, volume 323 of *A Series of Comprehensive Studies in Mathematics*. Springer, 2000.
- [Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, troisième édition, 1968.
- [Ser94] Jean-Pierre Serre. *Galois Cohomology*. Springer, 1994.