On the kernel of the norm in some unramified number fields extensions

Emmanuel Hallouin and Marc Perret*

February 1, 2008

Introduction

Let $L/K$ be a unramified Galois extension of number fields whose Galois group $G$ is a finite $p$-group ($p$ a prime integer). In [Ser94], Chap I, §4.4, it is proved that if $L$ is principal then:

$$d_pH^3(G,\mathbb{Z}) = d_pH^2(G,\mathbb{Z}/p\mathbb{Z}) - d_pH^1(G,\mathbb{Z}/p\mathbb{Z}) \leq r_1 + r_2$$

(1)

where $d_p G$ denotes the $p$-rank of a finite $p$-group $G$ and where $(r_1, r_2)$ is the signature of the number field $K$. Briefly, the proof works as follows. Let $C_L$ be the idèles class group of $L$ and $E_L$ its unit group, then:

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

The first isomorphism follows from the fact that $L$ is principal while the second one is part of class field theory. Thus:

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

(2)

The inequality (1) comes from the specialization at $q = -1$ of this isomorphism because the rank of $H^0(G, E_L)$ is easily bounded thanks to Dirichlet’s units theorem.

Together with Golod-Safarevich’s group theoretic result, (1) implies that if a number field $K$ satisfies the quadratic (in $d_p\mathcal{C}(K)$) inequality:

$$d_p\mathcal{C}(K)^2 - d_p\mathcal{C}(K) > r_1 + r_2 - 1$$

then its $p$-class field tower is infinite.

In order to find a cubic (in $d_p\mathcal{C}(K)$) analogue of this criteria, we specializes the isomorphism (2) at $q = -2$. This yields the following equality:

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

It is so crucial to find an upperbound for the $p$-rank $d_pH^{-1}(G, E_L)$ when $\mathcal{C}(L)$ is trivial. In this paper, we prove results about this rank in some special cases. More precisely, we compute this $p$-rank when $L/K$ is an abelian unramified (also at infinity) $p$-extension whose Galois group can be generated by two elements. We also exhibit an explicit basis of the $p$-group $H^{-1}(G, E_L)$.

Notations — Let $K$ be a number field. We denote by $\Sigma_K$ the set finite places, $\text{Div}(K)$ its divisor group and $\mathcal{C}(K)$ its divisor 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 divisor $\langle x \rangle_K$ 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 $w | v$) and $f_v$ the residual degree of any $w \in \Sigma_{L,v}$ over $K$. The map $e_{L/K} : \text{Div}(K) \to \text{Div}(L)$ is the classical extension of ideals.

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

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

in which we are interested (see [Ser68] for an introduction to the negative cohomology groups).

*Laboratoire Emile Picard, Institut de Mathématiques de Toulouse, France.
1 The cyclic case

Let \( L/K \) be a cyclic extension with Galois group \( G = \langle g \rangle \). A classical consequence of the Hilbert’s 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:

\[
H^1(G, L^*) = \{1\} \implies H^{-1}(G, L^*) = \{1\}.
\]

Another easy consequence already known is that:

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

\[
\varphi_g : \text{Ker}(\mathcal{C}(K) \to \mathcal{C}(L)) \to H^{-1}(G, E_L)
\]

\[
[I] \to \frac{g(y)}{y}
\]

where \([I]\) denotes the ideal class of \( I \) and \( y \) any generator of \( I \) in \( L \), is an isomorphism of groups.

**Proof** — The only non-trivial assertion to verify is the surjectivity of the map. Let \( u \in E_N[N_G] \), 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 an ideal \( I \) of \( K \): \( e_{L/K}(I) = \langle y \rangle_L \). Then \( u = \varphi_g([I]) \). \( \square \)

This proposition implies the following corollary:

**Corollary 2** Let \( K \) be a number field and \( L/K \) an unramified (included at infinity) abelian extension with Galois group \( G \) a cyclic \( p \)-group such that \( L \) is principal. If \( G = \langle g \rangle \) and if \( \pi \) generate a prime ideal of \( L \) with Frobenius equal to \( g \), then:

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

2 Some experiments with magma

With the help of magma and pari/gp, we have made some experiments and collect informations about the 2-rank of the group \( H^{-1}(G, E_{K_i}) \) 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 \( H^{-1}(E_{K^1}) \). If \( \mathcal{C}(K^1) \) is not trivial, we try to go further. We compute \( K^2 = (K^1)^\text{hilb} \) and the group structure of \( H^{-1}(E_{K^2}) \).

Here is our magma program we used:

```magma
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] ;
assert(I_G subset Ker_N) ;
printf "... structure of H^(-1)(G, E_M) = %o", 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 2·4 means that the concerning group is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \).

| \( \text{dis}(K) \) | \( \mathcal{C}_\ell(K) \) | \( \mathcal{C}_\ell(K^1) \) | \( H^{-1}(E_{K^1}) \) | \( \mathcal{C}_\ell(K^2) \) | \( H^{-1}(E_{K^2}) \) |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
|  -84            | 2·2             | 1               | 2·2·2           | 1               | 8               |
|  -120           | 2·2             | 2               | 4               | 1               | 8               |
|  -260           | 2·4             | 2               | 2·4             | 1               | 2·8             |
|  -280           | 2·2             | 4               | 4               | 1               | 16              |
|  -308           | 2·4             | 1               | 2·2·4           |                 |                 |
|  -399           | 2·8             | 1               | 2·2·8           |                 |                 |
|  -408           | 2·2             | 2               | 2·2·2           | 1               | 2·2·4           |
|  -420           | 2·2·2           | 2·2             | 2·2·2·4         | 1               | unknown         |

In the following section, we will explain why \( d_2H^{-1}(E_{K^1}) = 3 \) when \( d_2\mathcal{C}_\ell(K) = 2 \) and \( d_2\mathcal{C}_\ell(K^1) = 1 \). In all the remaining known cases, we point out that \( d_2H^{-1}(E_{K^1}) = d_2H^{-1}(E_{K^2}) \).

3 When the Galois group has two generators

The goal of is section is to extend the results of \[ \] to the case of extensions whose Galois group is an abelian group generated by two elements.

First, we 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 (included at infinity) extension whose Galois group \( G \) is an abelian \( p \)-group generated by two elements. Then \( H^{-1}(G, M^*) = 1 \).

**Proof** — Since \( M/K \) is an abelian unramified extension, there exists \( G' \) a subgroup of \( \mathcal{C}_\ell(K) \) such that \( G \cong \mathcal{C}_\ell(K)/G' \). Let \( p_1, \ldots, p_r \) be primes of \( K \) whose classes generate \( G' \). If \( G \cong \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/p^\beta\mathbb{Z} \) with \( \alpha \leq \beta \), we complete these primes by choosing \( p, q \) primes of \( K \) such that their decomposition groups in \( M/K \) satisfy \( D(p) = \langle (1, 1) \rangle \) and \( D(q) = \langle (0, 1) \rangle \). Adjoining \( p, q \) to the \( p_i \)'s leads to a system of generators of \( \mathcal{C}_\ell(K) \).

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

\[
\forall 1 \leq i \leq r, \quad D(p_i) \cap H = \{ \text{id} \}, \quad D(p) \cap H = \{ \text{id} \}, \quad D(q) \cap H = \{ \text{id} \}.
\]

Theorem 3 is implied by the following lemmas.

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

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

**Proof** — Suppose that \( H^{-1}(G, M^*) = \{ 1 \} \). 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, \( z \in M^*[N_G] = IG M^* \):

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

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 \( y \in IG \cdot H_M(z_1) \).

Conversely, suppose that \( H^{-1}(G/H, N_H(M^*)) = \{ 1 \} \). 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 \( z_1, \ldots, z_r \in M^* \) and \( g_1, \ldots, g_r \in G \) 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:

\[
z \in IG M^* \times M^*[N_H] = IG M^* \times IH M^* = IG M^*.
\]

because, \( H \) being cyclic, one has \( M^*[N_H] = IH M^* \). \( \square \)
Lemma 5 Let $H$ be a cyclic subgroup of $G$ such that $G/H$ is also cyclic. If $\mathcal{C}l(K)$ can be generated by primes whose decomposition groups intersect $H$ trivially, then $H^{-1}(G/H, N_{H}(M^{*})) = \{1\}$.

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:

$$\forall w \in \Sigma_{L}, w(y) \equiv 0 \pmod{f_{w}} \implies \forall w \in \Sigma_{L}, w \circ g(b) \equiv w(b) \pmod{f_{w}}$$

$$\implies \forall v \in \Sigma_{K}, \forall w, w' \in \Sigma_{L,v}, w'(b) \equiv w(b) \pmod{f_{w}}.$$ 

Note that there is no condition at infinity because infinite places are supposed unramified. 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, $\mathcal{C}l(K)$ can be generated by prime ideals $\mathfrak{p}_{1}, \ldots, \mathfrak{p}_{r}$ of $K$ whose decomposition groups satisfy $D(\mathfrak{p}_{i}) \cap H = \{1\}$. This means that all the primes of $L$ above the $\mathfrak{p}_{i}$ totally split in $M$. There exists $a \in K$ and $e_{1}, \ldots, e_{r} \in \mathbb{N}$ such that $(a) = I \times \prod_{i} \mathfrak{p}_{i}^{e_{i}}$. By construction, the ideal $ab$ of $L$ has support on primes of $L$ totally split in $M$.

Recall that, in a cyclic extension, the local-global principle is true form norm equations. Thus, by this local-global principle, 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. \hfill \square

Secondly, as in the cyclic case, one can ask if the triviality of the cohomological group with values in $M^{*}$ could imply some results about the cohomological group with values in $E_{M}$.

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

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

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

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

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

By duality, it is enough to compute the $p$-rank of $H^{4}(G, \mathbb{Z})$. This can be done, starting with the exact sequence of $G$-modules (trivial action) $0 \rightarrow \mathbb{Z} \overset{p}{\rightarrow} \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0$ and considering the long cohomology exact sequence:

$$0 \rightarrow H^{1}(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^{2}(G, \mathbb{Z}/p\mathbb{Z}) \overset{p}{\rightarrow} H^{2}(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow \cdots \rightarrow H^{3}(G, \mathbb{Z}/p\mathbb{Z}) \overset{p}{\rightarrow} H^{3}(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^{4}(G, \mathbb{Z})[p] \rightarrow 0.$$

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: $\#A[p] = p^{d_{p}-1}A$). 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 Künne’s formula (see [NSW00], exercice 7, page 96). \hfill \square
Let us return to the case where $d_p(G) = 2$. Then, due to proposition 3, one has $d_p(G, E_M) = 3$. As in corollary 2, one can be more precise and exhibit a basis of $H^{-1}(G, E_M)$.

**Theorem 7** Let $K$ be a number field and $M/K$ an unramified (included at infinity) abelian extension with Galois group $G$ a $p$-group of rank 2 such that $M$ is principal. If $G = \langle g_1, g_2 \rangle$ and if $\pi_1, \pi_2, \pi_{12}$ generate primes ideals of $M$ with Frobenius equal to $g_1, g_2$ and $g_1 g_2$ respectively, then:

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

**Proof — First step.** We claim that $H^{-1}(G, E_M)$ is generated by:

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

where $\sigma_\pi$ denotes the Frobenius at $\pi$.

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

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

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

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

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

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

Now start with $u \in E_M[N_G]$. By theorem 3, we know that $H^{-1}(G, M^*) = \{1\}$, i.e. $M^*[N_G] = I_G M^*$. Hence, there exists $z_1, z_2 \in M^*$ such that $u = \frac{\sigma_1(z_1) \sigma_2(z_2)}{z_2}$. Factorizing $z_1$ and $z_2$ into primes of $M$ of the form $\tilde{\sigma}(\pi_v)$, one shows that:

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

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

**Second step.** We consider a prime element $\pi$ of $M$ whose Frobenius is denoted by $\sigma_\pi$. Let us 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 $\frac{g_i(\pi)}{\pi}$ for $i = 1, 2, 12$.

To this end, put $H = \langle g_12 \rangle$, $L = M^H$ and $p = \langle \pi \rangle_M \cap K$, $p_1 = \langle \pi_1 \rangle_M \cap K$, $p_2 = \langle \pi_2 \rangle_M \cap K$.

There exists $\alpha_1, \alpha_2 \in \mathbb{N}$ such that $\sigma_\pi = g_1^\alpha g_2^\alpha$ and, by Artin map, $p = a^\alpha p_1^a p_2^\alpha$ with $a \in K^*$. Since $\langle \pi_i \rangle \cap H = \{1\}$ for $i = 1, 2$, the primes $p_i, i = 1, 2$, totally split between $L$ and $M$. Thus:

$$\begin{align*}
e_{L/K}(p) &= \langle N_H(\pi) \rangle_L, \\
e_{L/K}(p_i) &= \langle N_H(p_i) \rangle_L, i = 1, 2 \implies N_H(\pi) = av N_H(p_1)^{\alpha_1} N_H(p_2)^{\alpha_2},
\end{align*}$$

where $v \in E_L$. Hence:

$$N_H(u) = N_H \left( \frac{\sigma_\pi(\pi)}{\pi} \right) = \frac{\sigma_\pi(\pi)}{N_H(\pi)} = \frac{\sigma_\pi(a)}{\sigma_\pi(\pi)} \left( \frac{N_H(\pi)}{N_H(\pi)} \right)^{\alpha_1} = \left( \frac{N_H(\pi)}{\pi_1} \right)^{\alpha_1} \pi_2^{\alpha_2}.$$
Let us look separately, at 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 $\frac{\sigma_v(w)}{w}$ equals $N_H\left(\frac{\sigma_v(w)}{w}\right)$. 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 follow that:

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

where $w_1 \in E_M$. In conclusion, going back to $u$, it satisfies:

$$N_H(u) = N_H\left(\frac{\sigma_v(w_1)}{w_1} \frac{g_1(w_1)}{w_1} \frac{g_2(w_2)}{w_2} \left(\frac{g_1(\pi_1)}{\pi_1}\right)^{\alpha_1 \beta_1} \left(\frac{g_2(\pi_2)}{\pi_2}\right)^{\alpha_2 \beta_2}\right)$$

$$\implies u \times \left(\frac{\sigma_v(w_1)}{w_1} \frac{g_1(w_1)}{w_1} \frac{g_2(w_2)}{w_2} \left(\frac{g_1(\pi_1)}{\pi_1}\right)^{\alpha_1 \beta_1} \left(\frac{g_2(\pi_2)}{\pi_2}\right)^{\alpha_2 \beta_2}\right)^{-1} \in E_M[N_H].$$

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:

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

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**

[Len] Franz Lemmermeyer. A survey on class field towers, [http://www.fen.bilkent.edu.tr/~franz/publ.html](http://www.fen.bilkent.edu.tr/~franz/publ.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 edition, 1968.

[Ser94] Jean-Pierre Serre. *Galois Cohomology*. Springer, 1994.