ANNALES MATHÉMATIQUES

BLAISE PASCAL

Mohsen Asghari-Larimi and Abbas Movahhedi

# Bounds For Étale Capitulation Kernels II

Volume 16, n° 1 (2009), p. 151-163.

<http://ambp.cedram.org/item?id=AMBP_2009__16_1_151_0>



*Publication éditée par le laboratoire de mathématiques*
*de l'université Blaise-Pascal, UMR 6620 du CNRS*
*Clermont-Ferrand — France*

Annales mathématiques Blaise Pascal **16**, 151-163 (2009)

# Bounds For Étale Capitulation Kernels II

Mohsen Asghari-Larimi
Abbas Movahhedi

**Abstract**

Let $p$ be an odd prime and $E/F$ a cyclic $p$-extension of number fields. We give a lower bound for the order of the kernel and cokernel of the natural extension map between the even étale $K$-groups of the ring of $S$-integers of $E/F$, where $S$ is a finite set of primes containing those which are $p$-adic.

*Bornes pour les noyaux de capitulations II*

**Résumé**

Soit $p$ un nombre premier impair et $E/F$ une $p$-extension cyclique de corps de nombres. Nous donnons une minoration pour l'ordre du noyau et conoyau de l'application naturelle d'extension entre les $K$-groupes étales des anneaux de $S$-entiers de $E/F$ où $S$ est un ensemble fini de places contenant les places $p$-adiques.

## 1. Introduction

Let $F$ be an algebraic number field and let $p$ be an odd prime number. For a finite set $S$ of primes of $F$ containing the primes above $p$, let $o_F^S$ denote the ring of $S$-integers of $F$. For a Galois $p$-extension $E$ of $F$ with Galois group $G$ which is unramified outside $S$, the kernel and the cokernel of the natural functorial map between the even étale $K$-groups $f_i : K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow (K_{2i-2}^{\text{ét}}(o_E^S))^G$ are described by the cohomology of odd étale $K$-groups $K_{2i-1}^{\text{ét}}(o_E^S)$. So using Borel's results on the abelian group structure of odd $K$-groups, one can give an upper bound for the rank of the finite $p$-groups $\ker(f_i)$ and $\operatorname{coker}(f_i)$, as explained by B. KAHN [8, section 4], by means of the number of real and complex embeddings of the number field $F$. In [1], partially answering a question asked by B. KAHN *loc.cit.*, we gave a lower bound for the order of $\ker(f_i)$ and $\operatorname{coker}(f_i)$, in

*Keywords:* Capitulation, Tate kernel, K-group, Étale cohomology.
*Math. classification:* 11R70, 19F27.

the case where the extension $E/F$ is cyclic of degree $p$ in terms of tamely ramified primes. Our purpose in the present paper is to similarly treat the case where $E/F$ is cyclic of degree $p^n, n \geq 1$.

When the number field $F$ contains a primitive $p$-th root of unity $\zeta_p$, the classical Tate kernel $D_F$ consists of the non-zero elements $a$ of $F$, such that the symbol $\{a, \zeta_p\}$ is trivial in $K_2F$. Obviously, $D_F$ lies between $F^\bullet$, the multiplicative group of non zero elements of $F$ and $F^{\bullet p}$ . It is known that the factor group $D_F/F^{\bullet p}$ is of rank $1 + r_2$, where $r_2$ is the number of complex embeddings of $F$ [14]. When $F$ satisfies Leopoldt's conjecture at the prime $p$, the Kummer radical $A_F = A_F^{(1)}$ of the compositum of the first layers of $\mathbf{Z}_p$-extensions of $F$ has the same size : $A_F/F^{\bullet p} \cong D_F/F^{\bullet p}$. Answering a question raised by J. COATES [2], R. GREENBERG showed that even though in general $A_F \neq D_F$, they coincide when the base field $F$ contains enough $p$-primary roots of unity [4].

More generally, when $F$ contains the $p^n$-th roots of unity, for each integer $i \geq 2$, there exists a subgroup $D_F^{(i,n)}$ of $F^\bullet$ containing $F^{\bullet p^n}$, such that $K_{2i-1}^{\text{ét}}F/p^n \cong D_F^{(i,n)}/F^{\bullet p^n}$, and the order of $\text{coker}(f_i)$ is minorized by the norm index in the generalized Tate kernel $D_F^{(i,n)}$ (Proposition 2.1). Following Greenberg's method, one can show that, once again under Leopoldt's conjecture, $D_F^{(i,n)}$ turns out to be the Kummer radical $A_F^{(n)}$ of the compositum of the $n$-th layers of $\mathbf{Z}_p$-extensions of $F$, provided $F$ contains enough $p$-primary roots of unity. We then obtain our lower bound by minorizing the norm index $[A_F^{(n)} : A_F^{(n)} \cap N_{E/F}(E^\bullet)]$ in terms of the ramification indices in $E/F$ of non-$p$-adic primes belonging to the same "primitive" set for $(F, p)$ (Proposition 4.3).

At the end of the paper, we treat the case where the base field $F$ is "$p$-regular" and all the tamely ramified primes in $E/F$ belong to the same primitive set. In particular, we show that there are infinitely many cyclic extensions $E/F$ of degree $p^n$, such that the order of the kernel (or the cokernel) takes any prescribed value between 1 and the trivial upper bound $p^{n(1+r_2)}$.

## 2. A lower bound via the Tate kernel

Suppose that $E/F$ is a cyclic extension of degree $p^n$ with Galois group $G$, and that $F$ contains the $p^n$-th roots of unity $\mu_{p^n}$. Denote by $S$ the set of $p$-adic primes, as well as those which ramify in $E/F$. Throughout this paper $i$ is an integer $\geq 2$. The exact sequence

$$0 \to \mathbf{Z}_p(i) \to \mathbf{Z}_p(i) \to \mathbf{Z}/p^n\mathbf{Z}(i) \to 0$$

induces an injection

$$\begin{aligned} K_{2i-1}^{\text{ét}} F/p^n &\cong H^1(F, \mathbf{Z}_p(i))/p^n \\ &\hookrightarrow H^1(F, \mathbf{Z}/p^n\mathbf{Z}(i)) \\ &= H^1(F, \mu_{p^n})(i-1) \\ &\cong F^\bullet/F^{\bullet p^n}(i-1), \end{aligned}$$

where $H^1(F, \quad)$ denotes the first continuous cochain cohomology group of the absolute Galois group $G_F$ of $F$ and, for any $G_F$-module $M$, the notation $M(i)$ is the $i$-fold Tate twisted module $M$ [14].

Thus there exists a subgroup $D_F^{(i,n)}$ of $F^\bullet$ containing $F^{\bullet p^n}$ - the analogue of the Tate-kernel in the case of $i = 2$ and $n = 1$ -, such that

$$K_{2i-1}^{\text{ét}} F/p^n \cong (D_F^{(i,n)}/F^{\bullet p^n})(i-1).$$

Since the odd étale $K$-groups satisfy Galois descent, we have [1, Section 1]:

$$\begin{aligned} \operatorname{coker}(f_i) &\cong (K_{2i-1}^{\text{ét}} F/p^n)/N_{E/F}(K_{2i-1}^{\text{ét}} E/p^n) \\ &\cong D_F^{(i,n)}/F^{\bullet p^n} N_{E/F}(D_E^{(i,n)})(i-1). \end{aligned}$$

Since $F^{\bullet p^n} N_{E/F}(D_E^{(i,n)}) \subset D_F^{(i,n)} \cap N_{E/F}(E^\bullet)$, we have the following lower bound for the order of the kernel or the cokernel of the natural natural functorial map between the even étale $K$-groups

$$f_i : K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow (K_{2i-2}^{\text{ét}}(o_E^S))^G$$

(when $G$ is cyclic, the Herbrand quotient $h(G, K_{2i-1}^{\text{ét}}(o_E^S))$ is trivial, so that $\ker(f_i)$ and $\operatorname{coker}(f_i)$ have the same order):

**Proposition 2.1.** *Let $E/F$ be a cyclic extension of degree $p^n$ of algebraic number fields containing $\mu_{p^n}$. Then*

$$|\operatorname{coker}(f_i)| = |\ker(f_i)| \geq [D_F^{(i,n)} : D_F^{(i,n)} \cap N_{E/F}(E^\bullet)].$$

A detailed account of these generalized Tate kernels $D_F^{(i,n)}$ can be found in [6, 15], see also [9] for the case $n = 1$.

## 3. Tate kernel and Kummer radical

In this section, we fix a positive integer $n$ and assume that our base number field $F$ contains the $p^n$-th roots of unity $\mu_{p^n}$. Let $\mu_{p^\infty} := \cup_{m\geq 1}\mu_{p^m}$ be the group of all $p$-primary roots of unity and $F_\infty := F(\mu_{p^\infty})$ be the cyclotomic $\mathbf{Z}_p$-extension of $F$. Denote by $F_n$ the $n$-th layer in $F_\infty$ and by $\Gamma$ the Galois group $\mathrm{Gal}(F_\infty/F)$. Fix a topological generator $\gamma$ of $\Gamma$ in order to identify the Iwasawa algebra $\mathbf{Z}_p[[\Gamma]]$ with the power series algebra $\Lambda := \mathbf{Z}_p[[T]]$.

Let $\mathcal{K} := F_\infty^\bullet \otimes \mathbf{Q}_p/\mathbf{Z}_p$, considered as a discrete group on which $\Gamma$ acts through the first factor. Let $\tilde{F}$ be the compositum of all $\mathbf{Z}_p$-extensions of $F$ and

$$A_F^{(n)} = \{a \in F^\bullet / F(\sqrt[p^n]{a}) \subset \tilde{F}\}$$

be the Kummer radical of the compositum of the $n$-th layers of the $\mathbf{Z}_p$-extensions of $F$.

Following Greenberg [4],

$$A_F^{(n)} = \{a \in F^\bullet / a \otimes (p^{-n}\ mod\ \mathbf{Z}_p) \in \mathrm{Div}(\mathcal{K}(-1)^\Gamma)\}$$

and one can establish as in [1, page 204] that for all $i \geq 2$

$$D_F^{(i,n)} = \{a \in F^\bullet / a \otimes (p^{-n}\ mod\ \mathbf{Z}_p) \in \mathrm{Div}(\mathcal{K}(\mathrm{i}-1)^\Gamma)\}.$$

Here Div stands for the maximal divisible subgroup.

Let $K_\infty$ be the maximal abelian pro-$p$-extension of $F_\infty$. Kummer theory yields a perfect pairing [7, Section 7]

$$\begin{array}{ccc} \mathrm{Gal}(K_\infty/F_\infty) \times \mathcal{K} & \longrightarrow & \mu_{p^\infty} \\ (\sigma, a \otimes (p^{-m}\mathrm{mod}\ \mathbf{Z}_p)) & \longmapsto & \sigma(\sqrt[p^m]{a})/\sqrt[p^m]{a} \end{array}.$$

Now let $M_\infty$ be, as usual, the maximal abelian pro-$p$-extension of $F_\infty$ unramified outside $p$ and $\mathcal{X}_\infty := \mathrm{Gal}(M_\infty/F_\infty)$. Let $N_\infty$ be the subfield of $M_\infty$ fixed by the torsion submodule $\mathrm{Tor}_\Lambda(\mathcal{X}_\infty)$. Denote by $\mathcal{N}$ the subgroup of $\mathcal{K}$ corresponding to the field $N_\infty$ by the above pairing. For every integer $i$, we then have a perfect pairing

$$X(-i) \times \mathcal{N}(i-1) \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p,$$

where $X := \mathrm{Fr}_\Lambda \mathcal{X}_\infty = \mathrm{Gal}(N_\infty/F_\infty)$ is the maximal torsion-free quotient of $\mathcal{X}_\infty$.

It is well known that $X$ is a submodule of $\Lambda^{r_2}$ of finite index. The quotient module $H_F := \Lambda^{r_2}/X$ is isomorphic as an abelian group to the kernel of the natural map $K_2F_n \longrightarrow K_2F_\infty$, for $n$ large [2]. The exponent of the finite group $H_F$ will play an important role in what follows and will be henceforth denoted by $p^e$.

From the above pairing we see that for all $i \in \mathbf{Z}$, ${}_{p^n}\mathrm{Div}(\mathcal{N}(i-1)^\Gamma)$ is the Pontryagin dual of $\mathrm{Fr}_{\mathbf{Z}_p}(X(i)_\Gamma)/p^n$.

The following lemma generalizes [1, Lemma 2.1] to the case of cyclic extensions of degree $p^n$ with which we are dealing:

**Lemma 3.1.** *([4, page 1242]]) Let $j \equiv i \pmod{\mathrm{p^r}}$ for an integer $r \leq n+e$. Then*

$$\mathrm{Fr}_{\mathbf{Z}_p}(X(i)_\Gamma)/p^n = \mathrm{Fr}_{\mathbf{Z}_p}(X(j)_\Gamma)/p^n\ (i-j)$$

*provided $\mu_{p^{n+e-r}} \subset F$.*

*Proof.* As in the proof of [1, Lemma 2.1], we have, for each integer $i$,

$$\mathrm{Fr}_{\mathbf{Z}_p}(X(i)_\Gamma)/p^n \cong X(i)/(X(i) \cap T(\Lambda^{r_2}(i)) + p^nX(i)).$$

Let $Y_i := X(i) \cap T(\Lambda^{r_2}(i)) + p^nX(i)$. We have to show that the two submodules $Y_i$ and $Y_j$ are the same for any two integers $i$ and $j$ such that $j \equiv i \pmod{\mathrm{p^r}}$.

Let $\kappa$ be the cyclotomic character and recall that $\gamma$, which we have already fixed, is a topological generator of $\Gamma$. Denote the action of $T$ on $\Lambda^{r_2}(i)$ by $T^{(i)} := \kappa(\gamma)^i\gamma - 1$. Each element $y \in Y_i$ can be written as $y = T^{(i)}\lambda + p^nx$, with $T^{(i)}\lambda \in X$, for a $\lambda \in \Lambda^{r_2}$ and an $x \in X$. Write $y = (T^{(i)} - T^{(j)})\lambda + T^{(j)}\lambda + p^nx$. Since, by hypothesis $\mu_{p^{n+e-r}} \subset F$, we have

$$\kappa(\gamma) \equiv 1 (mod\, p^{n+e-r}).$$

Moreover $p^r$ dividing $i-j$, we obtain from the preceding congruence

$$\kappa(\gamma)^{i-j} \equiv 1 (mod\, p^{n+e}).$$

Thus $(T^{(i)} - T^{(j)})\Lambda^{r_2}$ is contained in $p^{n+e}\Lambda^{r_2}$. On the other hand, as an abelian group $X/Y_j \simeq (\mathbf{Z}/p^n\mathbf{Z})^{r_2}$ is of exponent $p^n$, so the exponent of $\Lambda^{r_2}/Y_j$ is at most $p^{n+e}$. Thus $(T^{(i)} - T^{(j)})\Lambda^{r_2} \subset Y_j$. The element $T^{(j)}\lambda$ of $T(\Lambda^{r_2}(j))$ is also in $X$ because $y$, $(T^{(i)} - T^{(j)})\lambda$ and $p^nx$ are in $X$. We conclude that $y$ is in $Y_j$. The lemma follows. □

By duality, the previous lemma then shows that under the same conditions

$$ {}_{p^n}\mathrm{Div}(\mathcal{N}(i)^{\Gamma}) = {}_{p^n}\mathrm{Div}(\mathcal{N}(j)^{\Gamma})(i-j). $$

In particular, putting $j = 0$:

$$ {}_{p^n}\mathrm{Div}(\mathcal{N}(i)^{\Gamma}) = {}_{p^n}\mathrm{Div}(\mathcal{N}^{\Gamma})(i). $$

Recall now that for any rational integer $i \geq 2$ [13]

$$ \mathrm{Div}(\mathcal{N}(\mathrm{i}-1)^{\Gamma}) = \mathrm{Div}(\mathcal{K}(\mathrm{i}-1)^{\Gamma}) $$

and for any $i \neq 1$ the above equality is conjectured to be true (Greenberg, Schneider). The case $i = 0$ corresponds to the Leopoldt conjecture for the base number field F at the prime $p$. Thus we have the following corollaries:

**Corollary 3.2.** *For two integers $i \geq 2$ and $j \geq 2$, if $j \equiv i \pmod{\mathrm{p}^{\mathrm{r}}}$ for an integer $r \leq n+e$, then*

$$ D_F^{(i,n)} = D_F^{(j,n)}(i-j) $$

*provided $\mu_{p^{n+e-r}} \subset F$. Recall our assumption that $F$ always contains at least $\mu_p$.*

In the following corollaries, we put $j = 0$ and $i \geq 2$.

**Corollary 3.3.** *Assume the number field $F$ contains $\mu_p$ and satisfies Leopoldt's conjecture at the prime $p$. Then*

$$ D_F^{(i,n)} = D_F^{(0,n)}(i) = A_F^{(n)}(i) $$

*provided $\mu_{p^{n+e-r}} \subset F$ for an integer $r \leq n+e$ such that $\mathrm{p}^{\mathrm{r}} \mid i$.*

Since $\mu_p \subset F$, for $m$ large, the $m$-th layer $F_m$ of the cyclotomic $\mathbf{Z}_p$-extension of $F$ contains enough $p$-primary roots of unity and the condition $\mu_{p^{n+e-r}} \subset F_m$ is automatically satisfied:

**Corollary 3.4.** *Assume that the layers $F_m$ of the cyclotomic $\mathbf{Z}_p$-extension of $F$ satisfy Leopoldt's conjecture at the prime $p$. Then, we have*

$$ D_{F_m}^{(i,n)} = D_{F_m}^{(0,n)}(i) = A_{F_m}^{(n)}(i) $$

*for $m$ large enough.*

The preceding corollaries generalize those of [1, Section 2] where the case of cyclic extensions of degree $p$ is treated.

## 4. Bounds For The Higher étale capitulation Kernels

Let $E/F$ be a cyclic extension of algebraic number fields of degree $p^n$, containing $\mu_{p^n}$, with Galois group $G$. The set $S$ consists of a finite set of primes containing $S_p$ and those primes which ramify in $E/F$. Since the étale $K$-groups $K_{2i-1}^{\text{ét}}F$ are finitely generated $\mathbf{Z}_p$-modules of rank $r_2$ and have cyclic torsion subgroup, we have the following upper bound for the kernel or the cokernel of the natural extension map $f_i : K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow (K_{2i-2}^{\text{ét}}(o_E^S))^G$:

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| \leq p^{n(1+r_2)},$$

where $i \geq 2$ and $r_2$ is the number of complex places of $F$.

We also recall that the maps $f_i$ are not injective once a non-$p$-adic prime ramifies in $E/F$ [1, Proposition 4.2].

Assume that the number field $F$ contains $\mu_{p^n}$. Let $\tilde{F}_n$ be the compositum of the $n$-th layers of the $\mathbf{Z}_p$-extensions of $F$. By the definition of the Kummer radical $A_F^{(n)}$, we have a perfect pairing

$$\begin{array}{ccc} \mathrm{Gal}(\tilde{F}_n/F) \times A_F^{(n)}/F^{\bullet p^n} & \longrightarrow & \mu_{p^n} \\ (\sigma, a) & \longmapsto & \sigma(\sqrt[p^n]{a})/\sqrt[p^n]{a}. \end{array}$$

**Definition 4.1.** ([3, 10, 11, 12]) A set $S$ of finite primes of $F$ containing $S_p$ is called primitive for $(F,\ p)$ if the Frobenius "attached" to the primes $v$ in $S-S_p$ generate a direct summand in $\mathrm{Gal}(\tilde{F}/F)$ of $\mathbf{Z}_p$-rank the cardinality of $S-S_p$, where $\tilde{F}$ is the compositum of all the $\mathbf{Z}_p$-extensions of $F$.

Let $S-S_p = \{v_1, v_2, \cdots, v_s\}$ be the set of non-$p$-adic primes which ramify in $E/F$. We extract from this a set $S_p \cup \{v_1, v_2, \cdots, v_t\}$ primitive for $(F,\ p)$. Denote by $\sigma_j := \sigma_j(\tilde{F}_n/F)$ the Frobenius "attached" to the prime $v_j$ in the extension $\tilde{F}_n/F$. We consider $\mathrm{Gal}(\tilde{F}_n/F)$ as a naturally free $\mathbf{Z}/p^n\mathbf{Z}$-module. By the definition of primitivity, the set $\{\sigma_1, \cdots, \sigma_t\}$ is $\mathbf{Z}/p^n\mathbf{Z}$-free and could be extended to a basis $\{\sigma_1, \cdots, \sigma_t, \sigma_{t+1}, \cdots, \sigma_{1+r_2+\delta_F}\}$ of $\mathrm{Gal}(\tilde{F}_n/F)$. Here $\delta_F$ dentoes the default of Leopoldt's conjecture for $(F,\ p)$. Introduce the dual basis $\{a_1, \cdots, a_{1+r_2+\delta_F}\}$ with respect to the above pairing:

$$\begin{cases} \sigma_j(\sqrt[p^n]{a_j}) = \zeta_{p^n} \sqrt[p^n]{a_j} & \text{for all} \quad j = 1, \cdots, 1+r_2+\delta_F \\ \sigma_j(\sqrt[p^n]{a_k}) = \sqrt[p^n]{a_k} & \text{whenever} \quad k \neq j. \end{cases}$$

Here $\zeta_{p^n}$ is a fixed primitive $p^n$-th root of unity. In particular, for each $j$, the prime $v_j$ remains inert in $F(\sqrt[p^n]{a_j})$ and splits in

$$F(\sqrt[p^n]{a_1}, \cdots, \sqrt[p^n]{a_{i-1}}, \sqrt[p^n]{a_{i+1}}, \cdots, \sqrt[p^n]{a_{1+r_2+\delta_F}}).$$

Let $v$ be any of the primes in $\{v_1, v_2, \cdots, v_t\}$. Denote by $w$ a prime of $E$ above $v$. Let $F_v, E_w$ be the completion of $F$ and $E$ at $v$ and $w$ respectively. The natural composite map $A_F^{(n)} \hookrightarrow F^\bullet \hookrightarrow F_v^\bullet$ induces the following injection

$$A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^\bullet) \hookrightarrow F_v^\bullet/N_{E_w/F_v}(E_w^\bullet) \cong Gal(E_w/F_v)$$

showing that $A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^\bullet)$ is cyclic. The following lemma gives the order of this cyclic group:

**Lemma 4.2.** *Let $v = v_j$ for a $j = 1, 2, \cdots, t$ and $w$ a prime of $E$ dividing $v$. Denote by $p^e \geq p$ the ramification index of $v$ in $E/F$. The factor group $A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^\bullet)$ is cyclic of order $p^e$.*

*Proof.* By construction, all the $a_k$ for $k \neq j$ belong to $N_{E_w/F_v}(E_w^\bullet)$ (since $\sqrt[p^n]{a_k} \in F_v$), so that $A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^\bullet)$ is generated by the class of $a = a_j$.

Let $E = F(\sqrt[p^n]{b})$. Let $( \, , \, )_v$ be the Hilbert symbol in the local field $F_v$ with values in $\mu_{p^n}$. For any integer $\alpha$, we have the following equivalences:

$$\begin{aligned} a^{p^\alpha} \in N_{E_w/F_v}(E_w^\bullet) &\iff (a^{p^\alpha}, b)_v = 1 \\ &\iff (a, b^{p^\alpha})_v = 1 \\ &\iff b^{p^\alpha} \in N_{F_v(\sqrt[p^n]{a})/F_v}(F_v(\sqrt[p^n]{a})). \end{aligned}$$

Since the extension $F_v(\sqrt[p^n]{a})/F_v$ is unramified of degree $p^n$, this last norm group consists of all elements whose valuation is exactly $p^n$. Accordingly, $a^{p^\alpha} \in N_{E_w/F_v}(E_w^\bullet)$ precisely when $p^{n-\alpha}$ divides the valuation of $b$ in $F_v$. Finally, we have: $a^{p^\alpha}$ is a norm in $E_w/F_v$ precisely when the local extension $F_v(\sqrt[p^{n-\alpha}]{b})/F_v$ is unramified.

Now, by definition of $e$, $F_v(\sqrt[p^{n-e}]{b})$ being the maximal unramified extension of $F_v$ contained in $E_w = F_v(\sqrt[p^n]{b})$, we conclude that the order of the class of $a$ in $A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^\bullet)$ is exactly $p^e$, as was to be shown. □

Now consider the canonical map

$$A_F^{(n)}/A_F^{(n)} \cap_{v\in T\setminus S_p} N_{E_w/F_v}(E_w^\bullet) \xrightarrow{\varphi} \prod_{v\in T\setminus S_p} A_F^{(n)}/A_F^{(n)} \cap N_{E_w/F_v}(E_w^\bullet)$$

where the set $T := S_p \cup \{v_1, v_2, \cdots, v_t\}$ consists of a primitive set for $(F,\ p)$ inside $S$. The map $\varphi$ is obviously injective. On the other hand, by the construction of the dual basis $a_j$, we have

$$\begin{cases} \varphi(\overline{a}_1) = (\overline{a}_1, 0, \cdots, 0) \\ \varphi(\overline{a}_2) = (0, \overline{a}_2, 0, \cdots, 0) \\ \cdots \\ \varphi(\overline{a}_t) = (0, \cdots, 0, \overline{a}_t). \end{cases}$$

Therefore, the map $\varphi$ is in fact an isomorphism. Now by the previous lemma, the target group is of order $p^{e_1+\cdots+e_t}$ where $p^{e_j} \geq p$ is the ramification index of the non-$p$-adic prime $v_j$ in the cyclic $p$-extension $E/F$. Accordingly

**Proposition 4.3.** *Let $E/F$ be a cyclic extension of degree $p^n$ containing $\mu_{p^n}$. Let $\{v_1, \cdots, v_t\}$ consist of a set of tamely ramified primes in $E/F$ belonging to a primitive set for $(F,\ p)$. We then have the following lower bound for the norm index in the Kummer radical $A_F^{(n)}$ of the $n$-th layers of the $\mathbf{Z}_p$-extensions of $F$ :*

$$[A_F^{(n)} : A_F^{(n)} \cap N_{E/F}(E^\bullet)] \geq p^{e_1+\cdots+e_t},$$

*where $p^{e_j}$ is the ramification index of $v_j$ in $E/F$.*

Combining this proposition with the results of the previous sections we get the following lower bound for the kernel or the cokernel of the natural map $f_i : K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow K_{2i-2}^{\text{ét}}(o_E^S)^G$, $i \geq 2$, which we are interested in.

**Theorem 4.4.** *Let $F$ be a number field satisfying Leopoldt's conjecture at the prime $p$. Let $E/F$ be a cyclic extension of degree $p^n$. Let $\{v_1, \cdots, v_t\}$ consist of a set of tamely ramified primes in $E/F$ belonging to a primitive set for $(F,\ p)$. Denote by $p^{e_j} \geq p$ the ramification index of $v_j$ in $E/F$ and by $p^e$ the exponent of $H_F$. Then*

$$|\ker(f_i)| = |\text{coker}(f_i)| \geq p^{e_1+\cdots+e_t},$$

*provided $\mu_{p^{n+e-r}} \subset F$ for an integer $r \leq n+e$ such that $p^r \mid i$.*

*Proof.* We successively have

$$
\begin{aligned}
|\ker(f_i)| = |\mathrm{coker}(f_i)| &\geq [D_F^{(i,n)} : D_F^{(i,n)} \cap N_{E/F}(E^\bullet)] \\
&= [A_F^{(n)} : A_F^{(n)} \cap N_{E/F}(E^\bullet)] \\
&\geq p^{e_1+\cdots+e_t}.
\end{aligned}
$$

□

In the classical case of $i = 2$, we necessarily have $r = 0$ and obtain:

**Corollary 4.5.** *Let $F$ be a number field satisfying Leopoldt's conjecture at the prime $p$ and let $\mu_{p^n} \subset F$. Let $E/F$ be a cyclic extension of degree $p^n$. Let $\{v_1, \cdots, v_t\}$ consist of a maximal set of tamely ramified primes in $E/F$ belonging to a primitive set for $(F,\ p)$. Denote by $p^{e_j} \geq p$ the ramification index of $v_j$ in $E/F$. If $\mu_{p^{n+e}} \subset F$, then we have the following lower bound*

$$|\ker(f)| = |\mathrm{coker}(f)| \geq p^{e_1+\cdots+e_t},$$

*for the kernel and the cokernel of the natural extension map of the tame kernels $f : K_2(o_F^S) \longrightarrow K_2(o_E^S)^G$.*

A set $T$ primitive for $(F,\ p)$ is said to be maximal when $T - S_p$ is as large as possible. When $F$ satisfies Leopoldt's conjecture, this is the case where $T - S_p$ contains exactly $1 + r_2$ primes, $r_2$ being the number of non-conjugate complex embeddings of $F$. When amongst totally and tamely ramified primes in $E/F$ one can extract a set $\{v_1, \cdots, v_{1+r_2}\}$ sitting in a primitive set, then the method developed here gives the exact size of $|\ker(f_i)| = |\mathrm{coker}(f_i)|$:

**Corollary 4.6.** *Let $F$ be a number field satisfying Leopoldt's conjecture at the prime $p$ and let $\mu_{p^n} \subset F$. Let $E/F$ be a cyclic extension of degree $p^n$. Assume there exists a primitive set $T$ for $(F,\ p)$ which is maximal, and such that each $v \in T - S_p$ is totally ramified in $E/F$. Then*

$$|\ker(f_i)| = |\mathrm{coker}(f_i)| = p^{n(1+r_2)},$$

*provided $\mu_{p^{n+e-r}} \subset F$ for an integer $r \leq n + e$ such that $p^r \mid i$.*

To finish, we establish that for each non-negative integer $t \leq 1 + r_2$, there exist cyclic extensions $E/F$ of degree $p^n$ where the order of $\ker(f_i)$ is exactly $p^{nt}$. Start with the following short exact sequence

$$0 \longrightarrow K_{2i-2}^{\text{ét}}(o_F) \longrightarrow K_{2i-2}^{\text{ét}}(o_F^S) \longrightarrow \oplus_{v\in S-S_p} H^2(F_v, \mathbf{Z}_p(i)) \longrightarrow 0.$$

We choose the ground number field $F$ to be $p$-regular (that is to say $K^{\text{ét}}_{2i-2}(o_F) = 0$). This is for example the case of any cyclotomic field $\mathbf{Q}(\mu_{p^n})$, provided the prime $p$ is regular. Furthermore, we suppose that the set $S$ is primitive for $(F,\ p)$ so that the number field $E$ is also $p$-regular. In this way, we get the following commutative diagramme

$$\begin{array}{ccc} K^{\text{ét}}_{2i-2}(o_E^S)^G & \overset{\sim}{\longrightarrow} & (\oplus_{v\in S-S_p}(\oplus_{w|v}H^2(E_w,\mathbf{Z}_p(i))))^G \\ f_i\uparrow & & \oplus_{v\in S-S_p}f_v\uparrow \\ K^{\text{ét}}_{2i-2}(o_F^S) & \overset{\sim}{\longrightarrow} & \oplus_{v\in S-S_p}H^2(F_v,\mathbf{Z}_p(i)) \end{array}$$

and all that remains to do is to estimate the order of the kernel of the right vertical map. For each prime $v$, by local duality, the kernel of $f_v$ has the same order as the cokernel of the canonical map

$$(\oplus_{w|v}H^0(E_w,\mathbf{Q}_p/\mathbf{Z}_p(1-i)))_G \longrightarrow H^0(F_v,\mathbf{Q}_p/\mathbf{Z}_p(1-i))$$

induced by the norm. Let $E'_w$ be the inertia field in $E_w/F_v$. Then $E'_w$ is obtained from $F_v$ by adjoining $p$-primary roots of unity (it is in fact a layer of the cyclotomic $\mathbf{Z}_p$-extension of $F_v$, namely $E'_w = F_{v,\infty}\cap E_w$). From this follows that the map

$$\oplus_{w|v}H^0(E'_w,\mathbf{Q}_p/\mathbf{Z}_p(1-i))) \longrightarrow H^0(F_v,\mathbf{Q}_p/\mathbf{Z}_p(1-i))$$

is in fact surjective, whereas in the totally ramified extension $E_w/E'_w$ the cokernel of the map

$$\oplus_{w|v}H^0(E_w,\mathbf{Q}_p/\mathbf{Z}_p(1-i))) \longrightarrow H^0(E'_w,\mathbf{Q}_p/\mathbf{Z}_p(1-i))$$

is of order $p^{e_v} = [E_w : E'_w]$, the ramification index of $v$ in $E/F$ (for details see [5, Lemma 4.2.1]).

Thus we have the following:

**Proposition 4.7.** *Let $F$ be a $p$-regular number field containing the $p^n$-th roots of unity and let $E/F$ be a cyclic extension of degree $p^n$. Then*

$$|\ \ker(f_i)\ |=|\ \mathrm{coker}(f_i)\ |= p^{\sum_{v\in S-S_p} e_v},$$

*provided the set $S$ of the $p$-adic prime of $F$ and those which ramify in $E$ is primitive for $(F,p)$.*

Čebotarev's density theorem guarantees that for each number field $F$ there exist infinitely many cyclic extensions $E$ of $F$ of degree $p^n$, such that the set $S$ of the $p$-adic primes of $F$ and the tamely ramified primes in $E/F$ is primitive for $(F,p)$, and such that each $v \in S - S_p$ has the prescribed ramified index $p^{e_v}$ in $E/F$. Thus, according to the preceding proposition, for each $p$-regular number field $F$ with $r_2$ non-conjugate complex embeddings, and for each $p$-power (given in advance) $p^m \leq p^{n(1+r_2)}$, we can find infinitely many cyclic extensions $E$ of $F$ of degree $p^n$, such that $\mid \ker(f_i) \mid = \mid \operatorname{coker}(f_i) \mid = p^m$.

## References


[1] J. Assim & A. Movahhedi – Bounds for étale capitulation kernels, *K-Theory* **33** (2004), no. 3, p. 199–213.

[2] J. Coates – On $K_2$ and some classical conjectures in algebraic number theory, *Ann. of Math. (2)* **95** (1972), p. 99–116.

[3] G. Gras & J.-F. Jaulent – Sur les corps de nombres réguliers, *Math. Z.* **202** (1989), no. 3, p. 343–365.

[4] R. Greenberg – A note on $K_2$ and the theory of $\mathbf{Z}_p$-extensions, *Amer. J. Math.* **100** (1978), no. 6, p. 1235–1245.

[5] R. A. Griffiths – A genus formula for étale hilbert kernels in a cyclic p-power extension, Thèse, McMaster University, 2005.

[6] K. Hutchinson – Tate kernels, étale k-theory and the gross kernel, Preprint, 2005.

[7] K. Iwasawa – On $\mathbf{Z}_l$-extensions of algebraic number fields, *Ann. of Math. (2)* **98** (1973), p. 246–326.

[8] B. Kahn – Descente galoisienne et $K_2$ des corps de nombres, *K-Theory* **7** (1993), no. 1, p. 55–100.

[9] M. Kolster & A. Movahhedi – Galois co-descent for étale wild kernels and capitulation, *Ann. Inst. Fourier (Grenoble)* **50** (2000), no. 1, p. 35–65.

[10] A. Movahhedi – Sur les $p$-extensions des corps $p$-rationnels, Thèse, Université Paris 7, 1988.

[11] ———, Sur les $p$-extensions des corps $p$-rationnels, *Math. Nachr.* **149** (1990), p. 163–176.

[12] A. Movahhedi & T. Nguyễ-Quang-Ḏỗ – Sur l'arithmétique des corps de nombres $p$-rationnels, in *Séminaire de Théorie des Nombres,*

*Paris 1987–88*, Progr. Math., vol. 81, Birkhäuser Boston, Boston, MA, 1990, p. 155–200.

[13] C. Soulé – $K$-théorie des anneaux d'entiers de corps de nombres et cohomologie étale, *Invent. Math.* **55** (1979), no. 3, p. 251–295.

[14] J. Tate – Relations between $K_2$ and Galois cohomology, *Invent. Math.* **36** (1976), p. 257–274.

[15] D. Vauclair – Capitulation, cup-produit et sous-modules finis dans les $\mathbf{z}_p$-extensions d'un corps de nombres, Preprint, Besançon, 2005.

Mohsen Asghari-Larimi
XLIM UMR 6172 CNRS
Mathématiques et informatique
Université de Limoges
123, Avenue A. Thomas
87060 Limoges Cedex
France

Abbas Movahhedi
XLIM UMR 6172 CNRS
Mathématiques et informatique
Université de Limoges
123, Avenue A. Thomas
87060 Limoges Cedex
France