TOKYO J. MATH.
VOL. 9, NO. 1, 1986

Decomposition and Inertia Groups in Z_p-Extensions

Georges GRAS

University of Franche-Comté-Besançon

(Communicated by K. Katase)

Introduction

In this paper, we shall give a canonical description of the decomposition and inertia groups, in a Z_p-extension of a number field k, for any prime ideal of k; when this prime ideal divides p, and ramifies in the Z_p-extension, all the higher ramification groups are also described. This description gives immediately a numerical knowledge of the previous groups, as soon as the p-class group and the group of units of k are numerically known.

Of course, if K/k is any abelian extension, the law of decomposition of prime ideals of k is known if and only if the Artin group of K/k is given; but in practice we have the opposite situation: the extension K/k is specified by mean of some property (for instance K/k is a Z_p-extension...) and the problem is to determine its Artin group. The results obtained in [2] give a general method for this kind of problem, via the use of a logarithm function, Log, which induces a canonical isomorphism between the Galois group G of the compositum $\tilde{k}$ of all Z_p-extensions of k, and an explicit Z_p-module attached to k and depending (numerically) on ideal classes and units. It is well known that the decomposition group $G_{\mathfrak{q}}$ in $\tilde{k}/k$, of any prime ideal $\mathfrak{q}$ of k, is the closure in G of the image of $k^\times$ by the Hasse norm residue symbol $((\ ,\tilde{k}/k)/\mathfrak{q})$; then it is sufficient to compute $\mathrm{Log}((a, \tilde{k}/k)/\mathfrak{q})$ for any $a \in k^\times$; we obtain an explicit formula for $\mathrm{Log}((a, \tilde{k}/k)/\mathfrak{q})$ which permits us to describe $G_{\mathfrak{q}}$ and its subgroups such as the inertia and higher ramification groups and to give some properties of jumps of ramification (§2). Finally, to illustrate this study, we consider (in §3) the case of imaginary quadratic fields and give all details for a numerical utilization.

Some basic tools used in this paper may be compared with some ones

Received January 21, 1985
Revised October 28, 1985

of T. Kubota [6] who first gave important insights in S-ramification aspects of class-field theory (see also some developments of Kubota's ideas in [8]). However, we think that the technics introduced in [2] and used here will give a new and more powerful approach for these questions.

I am pleased to thank Professor H. Miki for his remarks and suggestions about this paper, and Professor S. Iyanaga for his help concerning its publication.

§1. Canonical description of G.

We fixe a prime number p.

For any number field k, we denote by $\tilde{k}$ the compositum of all Z_p-extensions of k, and by G the Galois group $\mathrm{Gal}(\tilde{k}/k)$.

If K is any extension of k, contained in $\tilde{k}$, we know that the decomposition and inertia groups in K/k of a prime ideal of k, and more generally all its higher ramification groups (with upper numbering), are obtained by taking the restrictions of the corresponding groups in $\tilde{k}/k$ to K (see [1], chap. 11); then it is equivalent to solve the problem for $\tilde{k}$.

For any prime ideal $\mathfrak{q}$ of k we call:

$G_{\mathfrak{q}}$ the decomposition group of $\mathfrak{q}$ in $\tilde{k}/k$,

$G_{\mathfrak{q}}^0$ the inertia group of $\mathfrak{q}$ in $\tilde{k}/k$,

$G_{\mathfrak{q}}^i$, $i \geqq 0$, the higher ramification groups of $\mathfrak{q}$ in $\tilde{k}/k$ (with upper numbering).

As these groups are free Z_p-modules, they will be written additively.

We call S the set of prime ideals of k dividing p.

To recall the main result which gives a canonical description of G, we use the following notations concerning the field k:

(i) I, P, I_S, P_S are respectively the group of ideals, of principal ideals, of ideals prime to S, of principal ideals prime to S,

(ii) Z_k, E are respectively the ring of integers and the group of units,

(iii) $C_S = \prod_{\mathfrak{p} \in S} k_{\mathfrak{p}}$, $U_S = \prod_{\mathfrak{p} \in S} U_{\mathfrak{p}}$ are respectively the product of completions of k at $\mathfrak{p} \in S$ and the corresponding product of groups of local units; here, k is identified with its diagonal embedding in C_S,

(iv) $\log: U_S \rightarrow C_S$ is the usual p-adic logarithm (we have $\log = (\log_{\mathfrak{p}})_{\mathfrak{p} \in S}$, where $\log_{\mathfrak{p}}: U_{\mathfrak{p}} \rightarrow k_{\mathfrak{p}}$ is the classical extension of the $\mathfrak{p}$-adic logarithm on $U_{\mathfrak{p}}$),

(v) $B_S = C_S / V_S$, where $V_S = Q_p \log E$ is the Q_p-subspace of C_S generated by the logarithms of units of k,

(vi) $\mathrm{Log}: I_S \rightarrow B_S$ is the function defined by

$$\operatorname{Log} \mathfrak{a} = \frac{1}{n} \log a + V_S ,$$

where n is any integer such that $\mathfrak{a}^n = aZ_k$, $a \in k^\times$,

(vii) $\alpha: I_S \to G$ is the Artin map $(\alpha(\mathfrak{a}) = ((\tilde{k}/k)/\mathfrak{a}))$.

We know that Log is trivial on $\operatorname{Ker}\alpha$, and then may be defined on $\alpha(I_S)$, and finally on G (See [2], §2); the image of G by Log is $\overline{\operatorname{Log} I_S}$, the closure of $\operatorname{Log} I_S$ in B_S:

THEOREM 1.1. *The continuous map* $\operatorname{Log}: G \to \overline{\operatorname{Log} I_S}$, *defined on the dense subgroup* $\alpha(I_S)$ *of* G *by* $\operatorname{Log}\alpha(\mathfrak{a}) = \operatorname{Log}\mathfrak{a}$, *is a canonical isomorphism of* G *onto* $\overline{\operatorname{Log} I_S}$.

Now we identify G with $\overline{\operatorname{Log} I_S}$ and we will describe any subgroup of G in terms of the corresponding subgroup of $\overline{\operatorname{Log} I_S}$; for instance, if $k = Q$, the corresponding group G is qZ_p, where $q = p$ (resp. 4) if $p \neq 2$ (resp. $p = 2$).

Note that if H is any group of automorphisms of k, the groups G, C_S, U_S, V_S, B_S are canonically $Z_p[H]$-modules and Log an isomorphism of $Z_p[H]$-modules.

§2. Canonical description of $G_{\mathfrak{q}}$.

2.1. The tame case.

If the prime $\mathfrak{q} = \mathfrak{l}$ is not in S, then we have immediately the result because $\mathfrak{l}$ does not ramify and the Artin symbol $\alpha(\mathfrak{l})$ is a topological generator of $G_{\mathfrak{l}}$:

THEOREM 2.1. *If* $\mathfrak{l}$ *is a prime ideal of* k *which does not divide* p, *the decomposition group* $G_{\mathfrak{l}}$ *of* $\mathfrak{l}$ *in* $\tilde{k}/k$ *is* $G_{\mathfrak{l}} = Z_p \operatorname{Log} \mathfrak{l}$.

REMARK. As $\mathfrak{l}$ does not ramify, it is known that the Hasse norm residue symbol $((a, \tilde{k}/k)/\mathfrak{l})$, $a \in k^\times$, is given by $((\tilde{k}/k)/\mathfrak{l})^{-v_{\mathfrak{l}}(a)}$, where $v_{\mathfrak{l}}: k^\times \twoheadrightarrow Z$ is the $\mathfrak{l}$-adic valuation on $k^\times$; then we have, with the Log function:

$$\operatorname{Log}\left(\frac{a, \tilde{k}/k}{\mathfrak{l}}\right) = -v_{\mathfrak{l}}(a) \operatorname{Log} \mathfrak{l} ;$$

then, as the image of $k^\times$ by $((\ , \tilde{k}/k)/\mathfrak{l})$ is dense in $G_{\mathfrak{l}}$, we find again that $G_{\mathfrak{l}} = Z_p \operatorname{Log} \mathfrak{l}$.

2.2. The wild case.

If $\mathfrak{q} = \mathfrak{p} \in S$, then $\mathfrak{p}$ ramifies in $\tilde{k}/k$, and the description of $G_{\mathfrak{p}}$, $G_{\mathfrak{p}}^0$ and the higher ramification groups $G_{\mathfrak{p}}^i$, requires an extension of the Log function.

a) Extension of the Log function to I.

Let $\mathfrak{a} \in I$; if $\mathfrak{a}^n = aZ_k$, $a \in k^\times$, we will put $\mathrm{Log}\,\mathfrak{a} = (1/n)\log a + V_S$, in the same way as for elements of I_S; then we must define log on $k^\times$: the more natural and efficient definition is that of Iwasawa ([5], §4.2):

Let $a \in k^\times$ and $\log = (\log_\mathfrak{p})_{\mathfrak{p} \in S}$ (in the usual sense); if we consider a in $k_\mathfrak{p}^\times$ then there exists integers $e > 0$ such that $a^e = p^\lambda u$, $\lambda \in Z$, $u \in U_\mathfrak{p}$, and we put:

$$\log_\mathfrak{p} a = \frac{1}{e} \log_\mathfrak{p} u$$

(equivalently we put $\log_\mathfrak{p} p = 0$ for each $\mathfrak{p} \in S$).

The properties of Iwasawa's log function show that $\mathrm{Log}: I \to B_S$ is an homomorphism of groups.

Remark. It must be noted that for any $\mathfrak{m} \in \langle S \rangle$ the value $\mathrm{Log}\,\mathfrak{m}$ is defined in B_S but is not, in general, in $\overline{\mathrm{Log}\, I_S}$.

b) Class field theory.

As the Artin map is not defined in $\tilde{k}/k$ for $\mathfrak{p} \in S$, we use Hasse norm residue symbol, whose main properties are the following ones:

(i) the image of $k^\times$ by $((\ ,\tilde{k}/k)/\mathfrak{p})$ is a dense subgroup of $G_\mathfrak{p}$;

(ii) more generally, if $k^i_{(\mathfrak{p})}$, $i \geq 0$, is the subgroup $k^\times \cap U^i_\mathfrak{p}$, where $\{U^i_\mathfrak{p}\}_{i \geq 0}$ is the usual filtration of the group $U_\mathfrak{p}$, then the image of $k^i_{(\mathfrak{p})}$ by $((\ ,\tilde{k}/k)/\mathfrak{p})$ is a dense subgroup of the i-th higher ramification group $G^i_\mathfrak{p}$ (in upper numbering). Of course, as G is a pro-p-group, we have $G^0_\mathfrak{p} = G^1_\mathfrak{p}$ for all $\mathfrak{p} \in S$.

Then the problem is reduced to the computation of $((a, \tilde{k}/k)/\mathfrak{p})$, for $a \in k^\times$ and $\mathfrak{p} \in S$.

c) Computation of $((a, \tilde{k}/k)/\mathfrak{p})$.

Let a be an element of $k^\times$ and let $\mathfrak{p} \in S$. Let $aZ_k = \mathfrak{p}^{v_\mathfrak{p}(a)}\mathfrak{a}$, $\mathfrak{a} \in I$, $\mathfrak{a}$ prime to $\mathfrak{p}$; we recall that $((a, \tilde{k}/k)/\mathfrak{p})$ may be approximated by a suitable Artin symbol in the following manner:

Let $\mathfrak{m} = \mathfrak{p}^{-1} \prod_{\mathfrak{q} \in S} \mathfrak{q}$, and let n be any large enough integer ($n > v_\mathfrak{p}(a)$ for instance), and let $b_n \in k^\times$ be such that the two following multiplicative congruences are satisfied:

$$b_n \equiv a \bmod^\times \mathfrak{p}^n$$
$$b_n \equiv 1 \bmod^\times \mathfrak{m}^n\ ;$$

then if we put $b_n Z_k = \mathfrak{p}^{v_\mathfrak{p}(b_n)}\mathfrak{b}_n$, $\mathfrak{b}_n \in I$, we see that $v_\mathfrak{p}(b_n) = v_\mathfrak{p}(a)$ and that

$\mathfrak{b}_n \in I_S$. Then $\sigma_n = ((\boldsymbol{a}, \tilde{\boldsymbol{k}}/\boldsymbol{k})/\mathfrak{p})((\tilde{\boldsymbol{k}}/\boldsymbol{k})/\mathfrak{b}_n)^{-1} \in \mathrm{Gal}(\tilde{\boldsymbol{k}}/\boldsymbol{k}^{(n)})$ where $\boldsymbol{k}^{(n)}$ is the ray class field $\mathrm{mod}(\prod_{\mathfrak{q}\in S}\mathfrak{q})^n$; then $\sigma_n \to 1$ in G as $n \to \infty$.

We have $\mathrm{Log}((\boldsymbol{a}, \tilde{\boldsymbol{k}}/\boldsymbol{k})/\mathfrak{p})$ which is approximated by $\mathrm{Log}\,\mathfrak{b}_n$; but, by using the extension of Log to I, described in §a, we have $\mathrm{Log}\,\mathfrak{b}_n = \mathrm{Log}\,\boldsymbol{b}_n - v_{\mathfrak{p}}(\boldsymbol{a})\mathrm{Log}\,\mathfrak{p}$, and we see the following facts:

(i) if $\mathfrak{q} \in S$, $\mathfrak{q} \neq \mathfrak{p}$, then $\log_{\mathfrak{q}} \boldsymbol{b}_n$ is close to 0;

(ii) if $\mathfrak{q} = \mathfrak{p}$, then $\log_{\mathfrak{q}} \boldsymbol{b}_n$ is close to $\log_{\mathfrak{p}} \boldsymbol{a}$; then $\mathrm{Log}\,\boldsymbol{b}_n$ is close to $(\log_{\mathfrak{p}} \boldsymbol{a}, 0, \cdots, 0) + V_S$; then finally we obtain:

THEOREM 2.2. *For any $\boldsymbol{a} \in \boldsymbol{k}^\times$ and $\mathfrak{p} \in S$, the canonical image of $((\boldsymbol{a}, \tilde{\boldsymbol{k}}/\boldsymbol{k})/\mathfrak{p}) \in G$ in $\overline{\mathrm{Log}\,I_S}$ is given by*:

$$\mathrm{Log}\left(\frac{\boldsymbol{a}, \tilde{\boldsymbol{k}}/\boldsymbol{k}}{\mathfrak{p}}\right) = (\log_{\mathfrak{p}} \boldsymbol{a}, 0, \cdots, 0) - v_{\mathfrak{p}}(\boldsymbol{a})\mathrm{Log}\,\mathfrak{p}\ .$$

REMARK. Let $\boldsymbol{a} \in \boldsymbol{k}^\times$. Then we have (See §2.1)

$$\begin{aligned}\sum_{\mathfrak{q}} \mathrm{Log}\left(\frac{\boldsymbol{a}, \tilde{\boldsymbol{k}}/\boldsymbol{k}}{\mathfrak{q}}\right) &= \sum_{\mathfrak{q}\in S} \mathrm{Log}\left(\frac{\boldsymbol{a}, \tilde{\boldsymbol{k}}/\boldsymbol{k}}{\mathfrak{q}}\right) + \sum_{\mathfrak{q}\notin S} \mathrm{Log}\left(\frac{\boldsymbol{a}, \tilde{\boldsymbol{k}}/\boldsymbol{k}}{\mathfrak{q}}\right)\\ &= (\log_{\mathfrak{p}} \boldsymbol{a})_{\mathfrak{p}\in S} - \sum_{\mathfrak{q}\in S} v_{\mathfrak{q}}(\boldsymbol{a})\mathrm{Log}\,\mathfrak{q} - \sum_{\mathfrak{q}\notin S} v_{\mathfrak{q}}(\boldsymbol{a})\mathrm{Log}\,\mathfrak{q}\\ &= \mathrm{Log}\,\boldsymbol{a} - \mathrm{Log}\,\boldsymbol{a} = 0\ .\end{aligned}$$

Of course this phenomena means the product formula.

d) The decomposition group $G_{\mathfrak{p}}$.

To obtain $G_{\mathfrak{p}}$ it is sufficient to compute the sub-Z_p-module generated in B_S by the elements $(\log_{\mathfrak{p}} \boldsymbol{a}, 0, \cdots, 0) - v_{\mathfrak{p}}(\boldsymbol{a})\mathrm{Log}\,\mathfrak{p}$, when $\boldsymbol{a}$ varies in $\boldsymbol{k}^\times$; we obtain:

THEOREM 2.3. *The decomposition group $G_{\mathfrak{p}}$ of $\mathfrak{p} \in S$ in $\tilde{\boldsymbol{k}}/\boldsymbol{k}$ is*:

$$G_{\mathfrak{p}} = ((\log_{\mathfrak{p}} \pi_{\mathfrak{p}}, 0, \cdots, 0) - \mathrm{Log}\,\mathfrak{p})Z_p + (\log_{\mathfrak{p}} U_{\mathfrak{p}}) \times \{0\} \times \cdots \times \{0\} + V_S/V_S\ ,$$

where $\pi_{\mathfrak{p}}$ is any prime element in $\boldsymbol{k}_{\mathfrak{p}}$.

PROOF.

We can choose $\pi_{\mathfrak{p}}$ in $\boldsymbol{k}^\times$.

Let $\boldsymbol{a} \in \boldsymbol{k}^\times$; considering $\boldsymbol{a}$ in $\boldsymbol{k}_{\mathfrak{p}}^\times$, we have $\boldsymbol{a} = \pi_{\mathfrak{p}}^\lambda \boldsymbol{u}$, $\lambda \in Z$, $\boldsymbol{u} \in \boldsymbol{k}^\times \cap U_{\mathfrak{p}}$, and $\mathrm{Log}((\boldsymbol{a}, \tilde{\boldsymbol{k}}/\boldsymbol{k})/\mathfrak{p}) = (\log_{\mathfrak{p}} \boldsymbol{a}, 0, \cdots, 0) - v_{\mathfrak{p}}(\boldsymbol{a})\mathrm{Log}\,\mathfrak{p} = (\lambda \log_{\mathfrak{p}} \pi_{\mathfrak{p}} + \log_{\mathfrak{p}} \boldsymbol{u}, 0, \cdots, 0) - \lambda\,\mathrm{Log}\,\mathfrak{p} = \lambda((\log_{\mathfrak{p}} \pi_{\mathfrak{p}}, 0, \cdots, 0) - \mathrm{Log}\,\mathfrak{p}) + (\log_{\mathfrak{p}} \boldsymbol{u}, 0, \cdots, 0) + V_S$. Conversely, as $\lambda \in Z$ and $\boldsymbol{u} \in \boldsymbol{k}^\times \cap U_{\mathfrak{p}}$ may be choosen independently, and by the fact that Z (resp. $\boldsymbol{k}^\times \cap U_{\mathfrak{p}}$) is dense in Z_p (resp. $U_{\mathfrak{p}}$), the result follows easily.

COROLLARY. *Let $\tilde{H}^S$ the maximal subextension of $\tilde{\boldsymbol{k}}$ which is unrami-*

fied on $\boldsymbol{k}$ and such that $\boldsymbol{S}$ splits completely (i.e. *in which all $\mathfrak{p} \in \boldsymbol{S}$ split completely*). *Then the field $\tilde{\boldsymbol{H}}^S$ is fixed by the subgroup*

$$(\mathrm{Log}\langle \boldsymbol{S}\rangle + \mathrm{Log}\, \boldsymbol{k}^\times) \cap \overline{\mathrm{Log}\, \boldsymbol{I}_S}$$

of $\overline{\mathrm{Log}\, \boldsymbol{I}_S}$.

Of course $\tilde{\boldsymbol{H}}^S$ is fixed by the subgroup of $\boldsymbol{G}$ generated by all the $\boldsymbol{G}_\mathfrak{p}$, $\mathfrak{p} \in \boldsymbol{S}$; then it is the subgroup:

$$\sum_{\mathfrak{p} \in S} ((0, \cdots, 0, \log_\mathfrak{p} \pi_\mathfrak{p}, 0, \cdots, 0) - \mathrm{Log}\, \mathfrak{p})\boldsymbol{Z}_p + \mathrm{Log}\, \boldsymbol{U}_S + \boldsymbol{V}_S / \boldsymbol{V}_S \ .$$

It is not difficult to prove the equality.

Remark 1. This result is consistent with the following situation of class field theory: Let $\boldsymbol{H}$ be the Hilbert $\boldsymbol{p}$-class field of $\boldsymbol{k}$ and let $\boldsymbol{H}^S$ be the maximal subfield of $\boldsymbol{H}$ where $\boldsymbol{S}$ splits completely, and put $\tilde{\boldsymbol{H}} = \tilde{\boldsymbol{k}} \cap \boldsymbol{H}$, $\tilde{\boldsymbol{H}}^S = \tilde{\boldsymbol{k}} \cap \boldsymbol{H}^S$. Then in the canonical isomorphism $\mathrm{Gal}(\boldsymbol{H}/\boldsymbol{k}) \simeq \boldsymbol{I}/\boldsymbol{P}$ (the class group $\mathscr{C}$) we have $\mathrm{Gal}(\boldsymbol{H}/\boldsymbol{H}^S) \simeq \{\mathfrak{m}\boldsymbol{P}, \mathfrak{m} \in \langle \boldsymbol{S}\rangle\}$ (denoted by $\mathscr{C}(\boldsymbol{S})$) and therefore $\mathrm{Gal}(\boldsymbol{H}^S/\boldsymbol{k}) \simeq \boldsymbol{I}/\langle \boldsymbol{S}\rangle\ \boldsymbol{P} \simeq \mathscr{C}/\mathscr{C}(\boldsymbol{S})$ (the $\boldsymbol{S}$-class group $\mathscr{C}^S$).

Remark 2. Suppose that we write $\mathfrak{p}^h = \omega Z_k$, $\omega \in \boldsymbol{k}^\times$, and $\omega = \pi_\mathfrak{p}^h w$, $w \in \boldsymbol{U}_\mathfrak{p}$; then a representative of $\mathrm{Log}\, \mathfrak{p}$ is $(1/h)\log \omega = \log \pi_\mathfrak{p} + (1/h)\log w$ and $(\log_\mathfrak{p} \pi_\mathfrak{p}, 0, \cdots, 0) - \mathrm{Log}\, \mathfrak{p}$ is represented by $(\log_\mathfrak{p} \pi_\mathfrak{p}, 0, \cdots, 0) - \log \pi_\mathfrak{p} - (1/h)\log w = (-(1/h)\log_\mathfrak{p} w, \cdots, -\log_\mathfrak{q} \pi_\mathfrak{p} - (1/h)\log_\mathfrak{q} w, \cdots)_{\mathfrak{q} \neq \mathfrak{p}}$.

This shows that we obtain a kind of local-global computation involving the class group (via the number h) and the local units via $\log_\mathfrak{p} \pi_\mathfrak{p}$; for instance, $(1/h)\log_\mathfrak{p} w$ is not necessarly in $\log_\mathfrak{p} \boldsymbol{U}_\mathfrak{p}$.

Example. Consider $\boldsymbol{k} = \boldsymbol{Q}(\sqrt{-15})$ and $\boldsymbol{p} = 2$; we have $\boldsymbol{S} = \{\mathfrak{p}, \mathfrak{q}\}$ and, as $\mathscr{C} \simeq \boldsymbol{Z}/2\boldsymbol{Z}$, we see that $\mathfrak{p}^2 = ((1+\sqrt{-15})/2)Z_k$; if we take $\pi_\mathfrak{p} = 2$, we have, in $\boldsymbol{k}_\mathfrak{p}$, $\omega = (1+\sqrt{-15})/2 = 4w$, where $w = (1+\sqrt{-15})/8 \in \boldsymbol{U}_\mathfrak{p}$; as $\sqrt{-15} \equiv -25 \bmod \mathfrak{p}^7$, we have $w \equiv -3 \bmod 16$, then $(1/2)\log_\mathfrak{p} w = 2u$, $u \in \boldsymbol{Z}_2^*$; we have also $(1/2)\log_\mathfrak{q} w = 2v$, $v \in \boldsymbol{Z}_2^*$. Then

$$\boldsymbol{G}_\mathfrak{p} = (2, 2)\boldsymbol{Z}_2 + (\log_\mathfrak{p} \boldsymbol{U}_\mathfrak{p}) \times \{0\} = (2, 2)\boldsymbol{Z}_2 \oplus (4, 0)\boldsymbol{Z}_2 \ .$$

As $\boldsymbol{G} = \overline{\mathrm{Log}\, \boldsymbol{I}_S} = \langle \mathrm{Log}\, \mathfrak{l}_3\rangle + \mathrm{Log}\, \boldsymbol{U}_S$ (where $\mathfrak{l}_3 | 3$ and $\mathfrak{l}_3^2 = 3Z_k$) we obtain

$$\boldsymbol{G} = (2, 2)\boldsymbol{Z}_2 \oplus (4, 0)\boldsymbol{Z}_2 \quad (= \boldsymbol{G}_\mathfrak{p} \text{ in this example}) \ .$$

e) The higher ramification groups.

We have recall in §b that $\boldsymbol{G}_\mathfrak{p}^i$, $i \geqq 0$, is the $\boldsymbol{Z}_p$-module generated by the $\mathrm{Log}((a, \tilde{k}/k)/\mathfrak{p})$, $a \in k^i_{(\mathfrak{p})}$, and the general computation of this symbol (See §c) gives immediately (of course, as G is a pro-p-group, we have $G^0_\mathfrak{p} = G^1_\mathfrak{p}$):

THEOREM 2.4. *For any $i \geqq 0$, the ramification group $G^i_\mathfrak{p}$ (in upper numbering) of $\mathfrak{p} \in S$ in $\tilde{k}/k$ is*:

$$G^i_\mathfrak{p} = (\log_\mathfrak{p} U^i_\mathfrak{p}) \times \{0\} \times \cdots \times \{0\} + V_S/V_S\ .$$

Now we give some remarks concerning the jumps of ramification in $\tilde{k}/k$.

Let $e_\mathfrak{p}$ be the absolute index of ramification of $\mathfrak{p}$. We know that if $i > e_\mathfrak{p}/(p-1)$, then $\log_\mathfrak{p}$: $U^i_\mathfrak{p} \to (\bar{\mathfrak{p}})^i$ is an isomorphism (where $\bar{\mathfrak{p}}$ denotes the closure of $\mathfrak{p}$ in the ring of integers of $k_\mathfrak{p}$).

Thus we deduce, from the previous description of $G^i_\mathfrak{p}$, the following results:

COROLLARY 1. *For $i > e_\mathfrak{p}/(p-1)$, $G^i_\mathfrak{p} = (\bar{\mathfrak{p}})^i \times \{0\} \times \cdots \times \{0\} + V_S/V_S$, and $G^{i+e_\mathfrak{p}}_\mathfrak{p} = pG^i_\mathfrak{p}$ (hence if $i > e_\mathfrak{p}/(p-1)$ is a jump of ramification of G, $i + e_\mathfrak{p}$ is also a jump of ramification).*

The case of a Z_p-extension is interesting and yields the following corollary (cf. Wyman [9]):

COROLLARY 2. *Let K/k be a Z_p-extension of k and let Γ be its Galois group. Then, for $i > e_\mathfrak{p}/(p-1)$, the set of jumps of ramification of Γ, for $\mathfrak{p} \in S$, is $\{i_0 + \lambda e_\mathfrak{p}, \lambda \in N\}$, where i_0 is the first jump$> e_\mathfrak{p}/(p-1)$.*

PROOF. Let $H = \mathrm{Gal}(\tilde{k}/K)$, and $\Gamma = G/H$. We know that $\Gamma^i_\mathfrak{p} = G^i_\mathfrak{p} H/H$ ([1], chap. 11, §2).

By the previous Corollary 1, if $i > e_\mathfrak{p}/(p-1)$ is a jump of Γ, $i + e_\mathfrak{p}$ is also a jump because $\Gamma^{i+e_\mathfrak{p}}_\mathfrak{p} = G^{i+e_\mathfrak{p}}_\mathfrak{p} H/H = pG^i_\mathfrak{p} H/H = p\Gamma^i_\mathfrak{p}$.

Let $m > n > e_\mathfrak{p}/(p-1)$ be two consecutive jumps of ramification of Γ. We prove now that $\Gamma^{n+1}_\mathfrak{p} = p\Gamma^n_\mathfrak{p}$ and $\Gamma^{m+1}_\mathfrak{p} = p\Gamma^m_\mathfrak{p}$. As $\Gamma_\mathfrak{p} \simeq Z_p$, if $\Gamma^{i+1}_\mathfrak{p} \neq \Gamma^i_\mathfrak{p}$, $i > e_\mathfrak{p}/(p-1)$, we have $\Gamma^{i+1}_\mathfrak{p} = p^\alpha \Gamma^i_\mathfrak{p}$, $\alpha \geqq 1$; but we have the surjection;

$$G^i_\mathfrak{p}/G^{i+1}_\mathfrak{p} \to G^i_\mathfrak{p} H/G^{i+1}_\mathfrak{p} H = \Gamma^i_\mathfrak{p}/\Gamma^{i+1}_\mathfrak{p}\ ,$$

and i must be a jump of G, but, as $G^{i+e_\mathfrak{p}}_\mathfrak{p} = pG^i_\mathfrak{p}$, this proves that $G^i_\mathfrak{p}/G^{i+1}_\mathfrak{p}$ is of exponent p and then $\Gamma^{i+1}_\mathfrak{p} = p\Gamma^i_\mathfrak{p}$. Therefore we have $\Gamma^{n+1}_\mathfrak{p} = p\Gamma^n_\mathfrak{p} = \Gamma^m_\mathfrak{p}$ and $\Gamma^{m+1}_\mathfrak{p} = p^2\Gamma^n_\mathfrak{p}$; then $G^n_\mathfrak{p}/G^{m+1}_\mathfrak{p}$ has the exponent p^2 at least; but as $G^{n+e_\mathfrak{p}}_\mathfrak{p} = pG^n_\mathfrak{p}$, it is necessary to have $m+1 > n + e_\mathfrak{p}$, then $m - n \geqq e_\mathfrak{p}$; we obtain $m = n + e_\mathfrak{p}$ as desired.

To compare these results with the local case, see [7] and the bibliography of this paper.

f) Some particular cases.

(i) If $\boldsymbol{p}$ does not split in $\boldsymbol{k}/\boldsymbol{Q}$, then as $\boldsymbol{p}Z_k=\mathfrak{p}^{e_\mathfrak{p}}$, we have $\mathrm{Log}\,\mathfrak{p}=(1/\boldsymbol{e}_\mathfrak{p})\mathrm{Log}\,\boldsymbol{p}=0$; but for a prime element π of $\boldsymbol{k}_\mathfrak{p}$, $\log\pi$ is not necessarily 0 (except for instance if $\mathfrak{p}$ is principal) (in this direction, we observe that if $\pi\in\boldsymbol{k}^\times$, $\pi Z_k=\mathfrak{p}\mathfrak{a}$, $\mathfrak{a}\in\boldsymbol{I}_S$, and then $\mathrm{Log}\,\pi=\mathrm{Log}\,\mathfrak{a}\in\overline{\mathrm{Log}\,\boldsymbol{I}_S}$). In this case we have:

$$\boldsymbol{G}_\mathfrak{p}=\boldsymbol{Z}_p\log\pi+\log\boldsymbol{U}_S+\boldsymbol{V}_S/\boldsymbol{V}_S\ ,$$

$$\boldsymbol{G}_\mathfrak{p}^i=\log\boldsymbol{U}_S^i+\boldsymbol{V}_S/\boldsymbol{V}_S\ ,\quad\text{for all}\quad \boldsymbol{i}\geqq 0\ .$$

(ii) If $\boldsymbol{p}$ does not ramify in $\boldsymbol{k}/\boldsymbol{Q}$, for any $\mathfrak{p}\in\boldsymbol{S}$ we may take $\pi_\mathfrak{p}=\boldsymbol{p}$, then $\log_\mathfrak{p}\pi_\mathfrak{p}=0$; but (except if $\boldsymbol{p}$ does not split, then is inert in $\boldsymbol{k}/\boldsymbol{Q}$) $\mathrm{Log}\,\mathfrak{p}$ is not necessarily 0.

In this case we have:

$$\boldsymbol{G}_\mathfrak{p}=\boldsymbol{Z}_p\,\mathrm{Log}\,\mathfrak{p}+(\log_\mathfrak{p}\boldsymbol{U}_\mathfrak{p})\times\{0\}\times\cdots\times\{0\}+\boldsymbol{V}_S/\boldsymbol{V}_S\ ,$$

$$\boldsymbol{G}_\mathfrak{p}^i=(\log_\mathfrak{p}\boldsymbol{U}_\mathfrak{p}^i)\times\{0\}\times\cdots\times\{0\}+\boldsymbol{V}_S/\boldsymbol{V}_S\ ,$$

for all $\boldsymbol{i}\geqq 0$.

g) Local norms.

If $\boldsymbol{K}$ is a finite extension of $\boldsymbol{k}$ contained in $\tilde{\boldsymbol{k}}$, we obtain an effective computation of $((\boldsymbol{a},\boldsymbol{K}/\boldsymbol{k})/\mathfrak{q})$ and a criterion for the condition "$\boldsymbol{a}\in\boldsymbol{k}^\times$ is a local norm at $\mathfrak{q}$ in $\boldsymbol{K}/\boldsymbol{k}$". For this we must know the Artin group $\boldsymbol{A}\subset\boldsymbol{I}_S$ of $\boldsymbol{K}(\boldsymbol{A}=\{\mathfrak{a}\in\boldsymbol{I}_S,\ ((\boldsymbol{K}/\boldsymbol{k})/\mathfrak{a})=1\})$; then $\mathrm{Gal}(\boldsymbol{K}/\boldsymbol{k})\simeq\overline{\mathrm{Log}\,\boldsymbol{I}_S}/\overline{\mathrm{Log}\,\boldsymbol{A}}$ ([2], corollary to Theorem 2.1.), and the map:

$$\begin{aligned}\boldsymbol{k}^\times &\longrightarrow \overline{\mathrm{Log}\,\boldsymbol{I}_S}/\overline{\mathrm{Log}\,\boldsymbol{A}}\\ \boldsymbol{a} &\longrightarrow \begin{cases} \qquad\qquad\qquad -\boldsymbol{v}_\mathfrak{q}(\boldsymbol{a})\mathrm{Log}\,\mathfrak{q}+\overline{\mathrm{Log}\,\boldsymbol{A}}\ , & \text{if}\quad \mathfrak{q}\notin\boldsymbol{S}\\ (\log_\mathfrak{q}\boldsymbol{a},0,\cdots,0)-\boldsymbol{v}_\mathfrak{q}(\boldsymbol{a})\mathrm{Log}\,\mathfrak{q}+\overline{\mathrm{Log}\,\boldsymbol{A}}\ , & \text{if}\quad \mathfrak{q}\in\boldsymbol{S}\end{cases}\end{aligned}$$

is, essentially, the Hasse norm residue symbol at $\mathfrak{q}$ in $\boldsymbol{K}/\boldsymbol{k}$, and its kernel gives the local norms at $\mathfrak{q}$ (cf. §2, c).

For instance this gives the elements $\boldsymbol{a}\in\boldsymbol{k}^\times$ which are local norms at $\mathfrak{q}$, in any finite subfield of $\tilde{\boldsymbol{k}}$.

This gives also (only for subfields of $\tilde{\boldsymbol{k}}$) a new approach concerning explicit reciprocity laws.

§3. The case of imaginary quadratic fields.

Such a situation offers many possibilities of numerical computations.

Let $k=Q(\sqrt{-m})$, m square free, be an imaginary quadratic field, and put $H=\{1, s\}=\mathrm{Gal}(k/Q)$. Such a field has two fundamental Z_p-extensions which are normal over Q (See [2], §3, or [4], §3): the cyclotomic one, $k_\infty=kQ_\infty$, for which the law of decomposition of prime ideals is rather trivial (because k_∞/Q is abelian), and the prodiedral one, F; we have $k_\infty F=\tilde{k}$, but, for $p=2$, $k_\infty \cap F$ is of degree 1 or 2 over k.

We call $\Gamma \simeq Z_p$ the Galois group $\mathrm{Gal}(F/k)$ (then H acts on Γ via the relation $s\gamma=-\gamma$, for all $\gamma \in \Gamma$).

As $\log E=0$, we have $B_S=C_S$ and then Log=log. We can then describe the subgroups of G corresponding to k_∞ and F (See [4], §3):

$$\mathrm{Gal}(\tilde{k}/k_\infty)=G^*=\overline{\log I_S}^* ,$$

the kernel of the trace map $C_S \to Q_p$ restricted to $\overline{\log I_S}$,

$$\mathrm{Gal}(\tilde{k}/F)=G^H=\overline{\log I_S}^H .$$

Of course, if $p\neq 2$, k_∞ and F are linearly disjoint over k and $\overline{\log I_S}^*=((1-s)/2)\overline{\log I_S}$, $\overline{\log I_S}^H=((1+s)/2)\overline{\log I_S}$; if $p=2$, we recall that $[k_\infty \cap F: k]=(2Z_2: \overline{\log I_S}^H)=2^\chi$, $\chi=0$ or 1 (See [4], Theorem 3.1 and its corollary).

Here we give only the results concerning the law of decomposition of prime ideals of k in F/k (the general case, in $\tilde{k}/k$, for the various Z_p-extensions, is obtained easily from the corresponding information in k_∞/k and, mainly, in F/k).

As $\Gamma \simeq Z_p$, all subfields of F are characterised by their degree over k. For this we suppose that $\overline{\log I_S}$ is numerically known (then $\overline{\log I_S}^*$, $\overline{\log I_S}^H$ and χ are known).

Remark. Let $\tilde{H}$ (resp. $\tilde{F}$) be the intersection of $\tilde{k}$ with the Hilbert p-class field H of k (resp. F); if $p\neq 2$, $\tilde{H}=\tilde{F}$ is the unique subfield of F of degree $(\overline{\log I_S}: \log U_S)$; if $p=2$, we have shown in [4] (See §2, pp. 13 and 14) how to find $\tilde{H}$ and $\tilde{F}$ (of course $[\tilde{H}: \tilde{F}]=1$ or 2).

We distinguish the tame and wild cases.

a) Tame case. Let $\mathfrak{q}=\mathfrak{l}\notin S$; the problem is to determine $(\Gamma: \Gamma_\mathfrak{l})$ which is given by the index $(G: G_\mathfrak{l}+G^H)$. We know (See §2) that $G_\mathfrak{l}=Z_p \log \mathfrak{l}$; then we have the following cases:

(i) if $\mathfrak{l}$ does not split in k/Q, $\mathfrak{l}^s=\mathfrak{l}$ and $G_\mathfrak{l}\subset G^H$, therefore $\mathfrak{l}$ splits completely in F.

(ii) if $\mathfrak{l}$ splits in k/Q, we have two cases:

–if $p\neq 2$, $G/Z_p \log \mathfrak{l}+G^H \simeq G^* \oplus G^H/Z_p \log \mathfrak{l}+G^H \simeq G^*/Z_p \log(\mathfrak{l}^{1-s})$, and $(\Gamma: \Gamma_\mathfrak{l})=(\overline{\log I_S}^*: Z_p \log \mathfrak{l}^{1-s})$.

–if $p=2$, we have the exact sequence:

$$1 \longrightarrow \boldsymbol{G}^*/\boldsymbol{G}^* \cap (\boldsymbol{Z}_2 \log \mathfrak{l} + \boldsymbol{G}^H) \longrightarrow \boldsymbol{G}/\boldsymbol{Z}_2 \log \mathfrak{l} + \boldsymbol{G}^H$$
$$\xrightarrow{\mathrm{Tr}} 4\boldsymbol{Z}_2/4 \times 2^{n(l)}\boldsymbol{Z}_2 + 4 \times 2^{\chi}\boldsymbol{Z}_2 \longrightarrow 1\ ,$$

where $l\boldsymbol{Z}_k = \mathfrak{l} \cap \boldsymbol{Z}$, and $\pm l = 1 + 4 \times 2^{n(l)}\boldsymbol{u}$, $\boldsymbol{u}$ odd.

Let $\sigma \in \boldsymbol{G}^*$ be such that $\sigma = \boldsymbol{a} \log \mathfrak{l} + \sigma_0$, $\boldsymbol{a} \in \boldsymbol{Z}_2$, $\sigma_0 \in \boldsymbol{G}^H$; then $0 = \boldsymbol{a} \log l + 2\sigma_0$, and $\sigma_0 = -(1/2)\boldsymbol{a} \log l$. As $\boldsymbol{G}^H = 2^{\chi+1}\boldsymbol{Z}_2$ and $\log l = 2^{n(l)+2}\boldsymbol{v}$, $\boldsymbol{v}$ odd, we must have $2^{1+n(l)}\boldsymbol{a} \in 2^{1+\chi}\boldsymbol{Z}_2$, therefore $\boldsymbol{a} \in 2^{\chi - n(l)}\boldsymbol{Z}_2 \cap \boldsymbol{Z}_2$; this is sufficient and gives $\boldsymbol{G}^* \cap (\boldsymbol{Z}_2 \log \mathfrak{l} + \boldsymbol{G}^H) = 2^{\mathrm{Max}(\chi - n(l), 0) - 1}\boldsymbol{Z}_2 \log \mathfrak{l}^{1-s}$.

Then we have the following values for $(\Gamma : \Gamma_{\mathfrak{l}})$:

	$\chi=0$	$\chi=1$
$n(l)=0$	$(\overline{\log \boldsymbol{Is}^*} : \frac{1}{2}\boldsymbol{Z}_2 \log \mathfrak{l}^{1-s})$	$(\overline{\log \boldsymbol{Is}^*} : \boldsymbol{Z}_2 \log \mathfrak{l}^{1-s})$
$n(l) \geqq 1$	$(\overline{\log \boldsymbol{Is}^*} : \frac{1}{2}\boldsymbol{Z}_2 \log \mathfrak{l}^{1-s})$	$(\overline{\log \boldsymbol{Is}^*} : \frac{1}{4}\boldsymbol{Z}_2 \log \mathfrak{l}^{1-s})$

The result does not depend on the choice of $\mathfrak{l} | l$.

b) Wild case. Let $\mathfrak{q} = \mathfrak{p} \in \boldsymbol{S}$; here the prime $\mathfrak{p}$ ramifies in $\boldsymbol{F}/\boldsymbol{k}$ and we must determine the groups $\Gamma_{\mathfrak{p}}$, $\Gamma_{\mathfrak{p}}^0$ (which do not depend on the choice of $\mathfrak{p} \in \boldsymbol{S}$); the decomposition field is contained in $\tilde{\boldsymbol{F}}$, and the inertia field is $\tilde{\boldsymbol{F}}$ which is known ([3], array III, p. 14). Then it remains to compute for instance $(\Gamma_{\mathfrak{p}} : \Gamma_{\mathfrak{p}}^0)$ which is the residual degree of $\mathfrak{p}$ in $\boldsymbol{F}/\boldsymbol{k}$; we see that $(\Gamma_{\mathfrak{p}} : \Gamma_{\mathfrak{p}}^0) = (\boldsymbol{G}_{\mathfrak{p}} + \boldsymbol{G}^H : \boldsymbol{G}_{\mathfrak{p}}^0 + \boldsymbol{G}^H) = (\boldsymbol{G}_{\mathfrak{p}} : \boldsymbol{G}_{\mathfrak{p}}^0 + \boldsymbol{G}_{\mathfrak{p}}^H)$ and we have the following cases:

(i) if $\mathfrak{p}$ is inert in $\boldsymbol{k}/\boldsymbol{Q}$, then (See case (ii) in §2, f) we have $\boldsymbol{G}_{\mathfrak{p}} = \boldsymbol{G}_{\mathfrak{p}}^0 = \log \boldsymbol{U}_S$, and therefore the decomposition field is also the inertia field $\tilde{\boldsymbol{F}}$.

(ii) if $\mathfrak{p}$ ramifies in $\boldsymbol{k}/\boldsymbol{Q}$ (See case (i) in §2, f) we have the following results:

—if $\boldsymbol{p} \neq 2$, then $\boldsymbol{p} | \boldsymbol{m}$ and we can take $\pi = \sqrt{-\boldsymbol{m}}$; then $\boldsymbol{G}_{\mathfrak{p}} = \boldsymbol{Z}_{\boldsymbol{p}} \log(\sqrt{-\boldsymbol{m}}) + \log \boldsymbol{U}_S = \log \boldsymbol{U}_S$; therefore the decomposition field is also $\tilde{\boldsymbol{F}}$.

—if $\boldsymbol{p} = 2$, we have $\boldsymbol{G}_{\mathfrak{p}} = \boldsymbol{Z}_2 \log \pi + \log \boldsymbol{U}_S$ where $\pi = \sqrt{-\boldsymbol{m}}$ if $\boldsymbol{m} \equiv 2 \bmod 4$, $\pi = 1 + \sqrt{-\boldsymbol{m}}$ if $\boldsymbol{m} \equiv 1 \bmod 4$. The computation of $\log \pi$ and that of $\log \boldsymbol{U}_S$ given in [3] (See array I, p. 10) give the following results concerning $\boldsymbol{G}_{\mathfrak{p}}$, and the index $(\boldsymbol{G}_{\mathfrak{p}} : \boldsymbol{G}_{\mathfrak{p}}^0 + \boldsymbol{G}_{\mathfrak{p}}^H) = (\boldsymbol{G}_{\mathfrak{p}} : \log \boldsymbol{U}_S + \boldsymbol{G}_{\mathfrak{p}}^H)$:

$\boldsymbol{k}_{\mathfrak{p}}$	$\boldsymbol{G}_{\mathfrak{p}}^0 = \log \boldsymbol{U}_S$	$\log \pi$ mod $\boldsymbol{G}_{\mathfrak{p}}^0$	$\boldsymbol{G}_{\mathfrak{p}}$	$(\Gamma_{\mathfrak{p}} : \Gamma_{\mathfrak{p}}^0)$
$\boldsymbol{Q}_2(\sqrt{-1})$	$(4)\oplus(2+2\sqrt{-1})$	0	$(4)\oplus(2+2\sqrt{-1})$	1
$\boldsymbol{Q}_2(\sqrt{-2})$	$(4)\oplus(2+\sqrt{-2})$	0	$(4)\oplus(2+\sqrt{-2})$	1
$\boldsymbol{Q}_2(\sqrt{-5})$	$(2)\oplus(2\sqrt{-5})$	$\sqrt{-5}$	$(2)\oplus(\sqrt{-5})$	2
$\boldsymbol{Q}_2(\sqrt{-6})$	$(4)\oplus(\sqrt{-6})$	2	$(2)\oplus(\sqrt{-6})$	1
$\boldsymbol{Q}_2(\sqrt{-10})$	$(4)\oplus(2+\sqrt{-10})$	2	$(2)\oplus(\sqrt{-10})$	1
$\boldsymbol{Q}_2(\sqrt{-14})$	$(4)\oplus(\sqrt{-14})$	0	$(4)\oplus(\sqrt{-14})$	1

In this array, (a) means aZ_p.

(iii) if $\mathfrak{p}$ splits in k/Q (See case (ii) in §2, f), then $G_{\mathfrak{p}}=Z_{\mathfrak{p}}\log\mathfrak{p}+\log_{\mathfrak{p}}U_{\mathfrak{p}}\times\{0\}$, $G_{\mathfrak{p}}^{0}=\log_{\mathfrak{p}}U_{\mathfrak{p}}\times\{0\}$:

—if $p\neq 2$, we recall that the inertia and decomposition fields of $\mathfrak{p}$ in F/k (resp. $\tilde{H}$ and $\tilde{H}^{S}$) do not depend on the choice of $\mathfrak{p}$; but $\tilde{H}$ is fixed by $\log_{\mathfrak{p}}U_{\mathfrak{p}}\times\{0\}+G^{H}=\log U_{S}$, and $\tilde{H}^{s}$ is fixed by $Z_{p}\log\mathfrak{p}+\log_{\mathfrak{p}}U_{\mathfrak{p}}\times\{0\}+G^{H}=Z_{p}\log\mathfrak{p}+\log U_{S}$; therefore $(\Gamma_{\mathfrak{p}}:\Gamma_{\mathfrak{p}}^{0})=(Z_{p}\log\mathfrak{p}+\log U_{S}:\log U_{S})=(Z_{p}\log\mathfrak{p}+pZ_{p}\times pZ_{p}:pZ_{p}\times pZ_{p})$.

—if $p=2$, the result of [4] (array III of Theorem 2.2) shows that $\tilde{H}/k$ is cyclic, and the final result depends on χ:

· if $\chi=0$, $[\tilde{H}:\tilde{F}]=2$, then $(\Gamma_{\mathfrak{p}}:\Gamma_{\mathfrak{p}}^{0})=(Z_{2}\log\mathfrak{p}+(4,0)Z_{2}+(2,2)Z_{2}:(4,0)Z_{2}+(2,2)Z_{2})$;

· if $\chi=1$, $\tilde{H}=\tilde{F}=k$, and in this case, $\Gamma_{\mathfrak{p}}=\Gamma_{\mathfrak{p}}^{0}=\Gamma$ ($\mathfrak{p}$ is totally ramified in F/k).

References

[1] E. Artin and J. Tate, Class Field Theory, W. A. Benjamin, New-York, 1967.

[2] G. Gras, Logarithme p-adique et groupes de Galois, J. Reine Angew. Math., **343** (1983), 64–80.

[3] G. Gras, Sur les Z_2-extensions d'un corps quadratique imaginaire, Ann. Inst. Fourier, vol. **33**, no. **4** (1983), 1–18.

[4] G. Gras, Logarithme p-adique, p-ramification abélienne et K_2, Séminaire de Théorie des Nombres, Bordeaux, Année 1982–1983, n°12.

[5] K. Iwasawa, Lectures on p-adic L-functions, Ann. of Math. Stud. **74**, Princeton University Press, Princeton, 1972.

[6] T. Kubota, Galois group of the maximal abelian extension of an algebraic number field, Nagoya Math. J., **12** (1957), 177–189.

[7] H. Miki, On the ramification numbers of cyclic p-extensions over local fields, J. Reine Angew. Math., **328** (1981), 99–115.

[8] H. Miki, On the maximal abelian l-extension of a finite algebraic number field with given ramification, Nagoya Math. J., **70** (1978), 183–202.

[9] B. F. Wyman, Wildly ramified gamma extensions, Amer. J. Math., **91** (1969), 135–152.

Present Address:
Université de Franche-Comté-Besançon
et C. N. R. S.
Faculté des Sciences
Mathématiques
U. A. 741
F-25030 Besançon Cedex
France