Groupe de travail
d'analyse ultramétrique

Georges Gras

# Logarithme $p$-adique et corps de classes

*Groupe de travail d'analyse ultramétrique*, tome 11 (1983-1984), exp. n° 6, p. 1-7

<http://www.numdam.org/item?id=GAU_1983-1984__11__A3_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
11e année, 1983/84, n° 6, 7 p.



28 novembre 1983

# LOGARITHME p-ADIQUE ET CORPS DE CLASSES

par Georges GRAS (*)

## Introduction.

Dans cet exposé, nous présentons un logarithme p-adique qui prolonge, en un certain sens, le logarithme usuel (et même le logarithme d'Iwasawa) ; bien sûr, le mot prolongement n'est pas à prendre au sens analytique mais au sens suivant .

Prenons un corps de nombres $k$ et posons $S = \{$idéaux premiers $\mathfrak{p}$ de $k$ divisant $p\}$ ; considérons

$C = \prod_{\mathfrak{p}\in S} k_{\mathfrak{p}}$ (produit des complétés de $k$ en $\mathfrak{p} \in S$ ),

$U = \prod_{\mathfrak{p}\in S} U_{\mathfrak{p}}$ (produit des groupes d'unités locales principales correspondant),

$\log : U \longrightarrow C$ (logarithme p-adique usuel $(\log_{\mathfrak{p}})_{\mathfrak{p}\in S}$ ),

$\mathrm{Log} : U \longrightarrow B = C/\mathbb{Q}_p \log E$ (où $\mathbb{Q}_p \log E$ est le $\mathbb{Q}_p$-sous-espace de $C$ engendré par $\log E$ , où $E$ est le groupe des unités (globales) de $k$ ).

Alors il existe un pro-p-groupe $G$ et une application (notée encore Log ) conduisant au diagramme exact suivant de $\mathbb{Z}_p$-modules ;

$$\begin{array}{ccccccccc} & & T' & \longrightarrow & T & & & & \\ & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & U/\overline{E} & \longrightarrow & G & \longrightarrow & Cl & \longrightarrow & 1 \\ & & \downarrow \mathrm{Log} & & \downarrow \log & & & & \\ 0 & \longrightarrow & \mathrm{Log}\, U & \longrightarrow & \mathrm{Log}\, G & & & & \end{array}$$

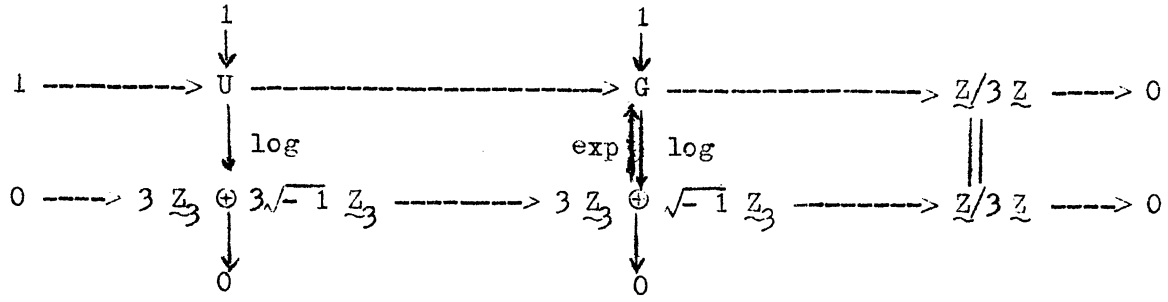
En fait le groupe $G$ est un groupe de Galois issu de la théorie du corps de classes, $T$ et $T'$ sont finis et $Cl$ est le p-groupe des classes de $k$ ; initialement le logarithme **Log** fut introduit pour décrire le groupe $G$ (et non l'inverse !).

Donnons un exemple numérique dans le seul cas (autre que $k = \mathbb{Q}$ ) où $\log E = 0$ (i. e. Log = log sur $U$ ), à savoir le cas des corps quadratiques imaginaires.

Pour $k = \mathbb{Q}(\sqrt{-439})$ et $p = 3$ (ce qui implique $C = \mathbb{Q}_3(\sqrt{-1})$ ), on obtient le schéma suivant :

---

(*) Georges GRAS, **CNRS, Equipe de Mathématiques U. A. 741**, et Université de Franche-Comté, 25030 BESANCON CEDEX.




Autrement dit, pour cette situation, il existe une exponentielle 3-adique définie sur un domaine qui contient des éléments de valeur absolue 1 , donc est strictement plus grand que le domaine usuel, qui serait ici

$$3\mathbb{Z}_3 \oplus 3\sqrt{-1}\,\mathbb{Z}_3 \subset \{x \in \mathbb{C}_3 \ , \ |x| < 3^{-1/3}\} \ ;$$

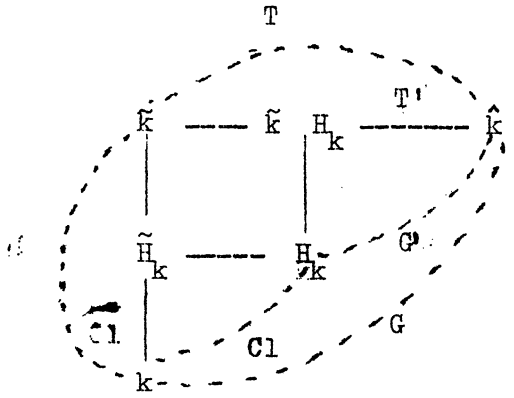
en contrepartie son image n'est pas dans U , mais il y a canonicité.

Nous allons maintenant définir G .

Pour certaines démonstrations, et pour les applications utilisant la fonction Log , on trouvera les détails, principalement dans nos articles [1], [2], [3].

1. Description de groupes de Galois.

Soit $\hat{k}$ la pro-p-extension abélienne maximale de k , p-ramifiée (i. e. non ramifiée en dehors de $S = \{\mathfrak{p} | p$ dans $k\}$ ). Elle conduit au schéma galoisien suivant




où $\tilde{k}$ est le composé des $\mathbb{Z}_p$-extensions de k :

$H_k$ est le p-corps de classes de Hilbert,

$\tilde{H}_k = \tilde{k} \cap H_k$ .

Le groupe $G = \mathrm{Gal}(\hat{k}/k)$ est un $\mathbb{Z}_p$-module de type fini dont le p-sous-groupe de torsion est le groupe fini $T = \mathrm{Gal}(\hat{k}/\tilde{k})$ .

Le groupe $\tilde{G} = \mathrm{Gal}(\tilde{k}/k) \simeq G/T$ est isomorphe à $\mathbb{Z}_p^\gamma$ , $\gamma \geqslant 1$ dépendant de la conjecture de Leopoldt ; mais on voudrait avoir un isomorphisme canonique entre $\tilde{G}$ et un $\mathbb{Z}_p$-module libre défini explicitement "dans k ", comme c'est le cas pour G' , qui est canoniquement isomorphe à $U/\mathbb{E}$ , tandis que G est décrit de la façon suivante,

via le symbole d'Artin.

Soit $I$ le groupe des idéaux de $k$ étrangers à $p$, soit $P_n$, $n \in \mathbb{N}$ le sous-groupe des idéaux principaux $(u)$ de $k$, où $u \equiv 1$ modulo $p^n$ (on pose $P_0 = P$, c'est le sous-groupe des idéaux principaux étrangers à $p$, et $I/P = Cl$ est le p-groupe des classes).

L'application d'Artin

$$\alpha : I \longrightarrow G$$

$$\mathfrak{a} \qquad \left(\left(\frac{F/k}{\mathfrak{a}}\right)\right)_{F, F \subset \hat{k}, [F:k]<\infty}$$

induit l'isomorphisme $\varprojlim_{n \in \mathbb{N}} I/P_n \simeq G$.

L'image $\alpha(I)$ est dense dans $G$.

On va voir alors que $\tilde{G}$ est une image logarithmique de $G$.

On a déjà defini dans l'introduction les objets suivants :

$$C\ ,\ U\ ,\ \log : U \longrightarrow C\ ,\quad \mathrm{Log} : U \to B = C/\mathbb{Q}_p \log E\ .$$

A ce stade, on prolonge Log à $I$ de la façon suivante :

$$\text{si } \mathfrak{a}^n = (a) \in P\ ,\ \text{on pose } \mathrm{Log}\ \mathfrak{a} = \frac{1}{n}\ \mathrm{Log}\ a \in B\ ;$$

on constate alors que Log est nul sur $\mathrm{Ker}\ \alpha$ (car $\mathrm{Ker}\ \alpha = \bigcap_{n \in \mathbb{N}} P_n$), ce qui induit une application continue de $\alpha(I)$ dans $B$ qui se prolonge donc à $G$ par continuité ; on appelle encore Log l'application qui en résulte ; comme $G$ est compact, on a :

$$\mathrm{Log}\ G = \overline{\mathrm{Log}\ I}\quad \text{(adhérence de Log I dans B)}.$$

Il n'est pas difficile alors de montrer que le noyau de Log dans $G$ est $T$, ce qui induit l'isomorphisme canonique que nous avions en vue

$$\tilde{G} \xrightarrow[\simeq]{\mathrm{Log}} \overline{\mathrm{Log}\ I}\ .$$

On en déduit alors facilement une description canonique des différents groupes de Galois figurant dans le schéma galoisien donné plus haut (et dont certains n'étaient pas "calculables" jusqu'à présent, comme $T = \mathrm{Gal}(\hat{k}/\tilde{k})$ et $\tilde{Cl} = \mathrm{Gal}(\tilde{H}_k/k)$ principalement).

COROLLAIRE 1. - On a $\tilde{Cl} \simeq \overline{\mathrm{Log}\ I}/\mathrm{Log}\ U$.

COROLLAIRE 2. - On a $|T| = (|Cl|/(\overline{\mathrm{Log}\ I} : \mathrm{Log}\ U))\ |T'|$ (où $|T'| = |\mathrm{tor}(U/\overline{E})|$ se calcule explicitement, et donne un terme essentiellement de la forme : Régulateur p-adique/Discriminant).

## 2. Exemple numérique.

Il est clair que dès que les classes d'idéaux et les unités de $k$ sont connues, on

peut calculer numériquement les invariants ci-dessus (notamment $\overline{\mathrm{Log}\ I}$ ).

Prenons $k = \mathbb{Q}(\sqrt{-439})$ , $p = 3$ . On a $E = \{\pm 1\}$ et $Cl \simeq \mathbb{Z}/3\mathbb{Z}$ .

On a $I = \langle I_{13} \rangle P$ , où $I_{13}$ est un idéal premier au dessus de 13 ; on obtient alors :

$$I_{13}^3 = (21 + 2\sqrt{-439}) ,$$

d'où

$$\overline{\mathrm{Log}\ I} = \langle \mathrm{Log}\ I_{13} \rangle + \mathrm{Log}\ U = \langle \mathrm{Log}\ I_{13} \rangle + 3\mathbb{Z}_3 \oplus 3\sqrt{-439}\ \mathbb{Z}_3 .$$

On a

$$\mathrm{Log}\ I_{13} = \frac{1}{3}\mathrm{Log}(21 + 2\sqrt{-439}) = \frac{1}{6}\mathrm{Log}(21 + 2\sqrt{-439})^2$$

$$= \frac{1}{6}\mathrm{Log}(-1 - 1314 + 84\sqrt{-439}) \equiv \sqrt{-439} \ \text{ modulo}(3) = \mathrm{Log}\ U ,$$

d'où $\overline{\mathrm{Log}\ I} = 3\mathbb{Z}_3 \oplus \sqrt{-439}\ \mathbb{Z}_3$ .

Dans ce cas on obtient :

$$\widetilde{Cl} \simeq \overline{\mathrm{Log}\ I}/\mathrm{Log}\ U \simeq \mathbb{Z}/3\mathbb{Z}$$

(ce qui signifie que l'on a $H_k \subset \tilde{k}$ : le 3-corps de classes de Hilbert est contenu dans le composé des $\mathbb{Z}_3$-extensions de $k$ ),

$$|T| = \frac{|Cl|}{(\overline{\mathrm{Log}\ I} : \mathrm{Log}\ U)} \quad |T'| = \frac{3}{3} = 1 \quad (\text{car } T' = 1)$$

(on obtient le schéma donné dans l'Introduction).

## 3. Autres applications.

L'existence de l'application Log a permis de résoudre les problèmes suivants.

(i) Structure galoisienne de $\tilde{G}$ : Si $H$ est un groupe d'automorphismes de $k$ , on peut expliciter la $\mathbb{Z}_p[H]$-structure de $\tilde{G}$ ;

(ii) On peut expliciter la loi de décomposition des idéaux premiers dans $\tilde{k}/k$ ;

(iii) Plongement kummérien dans $\tilde{k}$ : Si le groupe $\mu_p$ des racines $p$-ièmes de l'unité est contenu dans $k$ , et si les classes d'idéaux et les unités de $k$ sont connues, alors on peut trouver effectivement le sous-groupe maximal $\tilde{R}$ de $k^\times$ tel que $k(\sqrt[p]{\tilde{R}}) \subset \tilde{k}$ (i. e. le radical de l'extension de $k$ maximale d'exposant $p$ contenue dans $\tilde{k}$ ) ;

(iv) Propriétés de $K_2 k$ : Si $k$ satisfait à la conjecture de Leopoldt en $p$ , si $k$ contient le sous-corps réel maximal de $\mathbb{Q}(\mu_p)$ , alors on peut caractériser les $p$-extensions galoisiennes de $k$ dont la $p$-partie du noyau modéré (noyau dans $K_2 k$ du symbole modéré) est triviale.

Les points (iii) et (iv) étant plus techniques, nous renvoyons le lecteur aux deux articles [4], [5], où ces sujets sont traités en détail. Disons quelques mots des deux premiers.

(a) Structure galoisienne de $\tilde{G}$. - Limitons nous à l'exemple simple suivant (mais non trivial) des corps quadratiques imaginaires et $p = 2$. Soit

$$H = \{1 , s\} = \mathrm{Gal}(\mathbf{k}/\underset{\sim}{Q}) .$$

On sait que $\tilde{k}$ est le composé de deux $\underset{\sim}{Z}_2$-extensions canoniques :

$k_\infty$, la $\underset{\sim}{Z}_2$-extension cyclotomique de $k$,

$k'_\infty$, la $\underset{\sim}{Z}_2$-extension de $k$ prodiédrale sur $\underset{\sim}{Q}$.

On démontre facilement que $k_\infty$ est fixe par

$$\tilde{G}^* = \{g \in \tilde{G} , \ (i + s)\, g = 1\} ,$$

que $k'_\infty$ est fixe par

$$\tilde{G}^H = \{g \in \tilde{G} , \ (1 - s)\, g = 1\} .$$

Il est alors facile de voir que la $\underset{\sim}{Z}_2[H]$-structure de $\tilde{G}$ est entièrement caractérisée par le nombre suivant noté $2^\chi$ :

$$2^\chi = [k_\infty \cap k'_\infty : k] .$$

Plus précisément, on a le résultat suivant.

Si $\chi = 0$ ($k_\infty$ et $k'_\infty$ sont linéairement disjointes sur $k$) alors

$$\tilde{G} \simeq (1 + s)\, \underset{\sim}{Z}_2[H] \oplus (1 - s)\, \underset{\sim}{Z}_2[H] ;$$

Si $\chi = 1$ (non disjonction de $k_\infty$ et $k'_\infty$), alors

$$\tilde{G} \simeq \underset{\sim}{Z}_2[H] .$$

Le calcul de $\chi$ est alors standard en utilisant Log ; on a :

$$\begin{aligned} \mathrm{Gal}(k_\infty \cap k'_\infty/k) &\simeq \overline{\mathrm{Log}\ \bar{I}}/\overline{\mathrm{Log}\ \bar{I}}^H + \overline{\mathrm{Log}\ \bar{I}}^* \\ &\simeq (1 + s)\, \overline{\mathrm{Log}\ \bar{I}}/2\, \overline{\mathrm{Log}\ \bar{I}}^H \\ &\simeq \overline{\mathrm{Log}\ N_{k/\underset{\sim}{Q}}(\bar{I})}/2\, \overline{\mathrm{Log}\ \bar{I}}^H \\ &\simeq 2\, \underset{\sim}{Z}_2/\overline{\mathrm{Log}\ \bar{I}}^H . \end{aligned}$$

Exemple. - Si $k = \underset{\sim}{Q}(\sqrt{-82})$, on a $Cl \simeq \underset{\sim}{Z}/4\,\underset{\sim}{Z}$ ; on trouve

$$\overline{\mathrm{Log}\ \bar{I}} = 2\,\underset{\sim}{Z}_2 \oplus \sqrt{-82}\ \underset{\sim}{Z}_2 ,$$

d'où $\overline{\mathrm{Log}\ \bar{I}}^H = 2\,\underset{\sim}{Z}_2$, d'où $\chi = 0$.

Si $k = \underset{\sim}{Q}(\sqrt{-34})$, on a aussi $Cl \simeq \underset{\sim}{Z}/4\,\underset{\sim}{Z}$ ; mais en trouve :

$$\overline{\mathrm{Log}\ \bar{I}} = 4\,\underset{\sim}{Z}_2 \ominus (2 + \sqrt{-34})\ \underset{\sim}{Z}_2 ,$$

ce qui donne

$$\overline{\mathrm{Log}\ \bar{I}}^H = 4\,\underset{\sim}{Z}_2 \quad \text{et} \quad \chi = 1 .$$

On peut montrer que les $H$-modules $\widetilde{Cl} = \mathrm{Gal}(\tilde{H}_k/k) \simeq \overline{\mathrm{Log}\ \bar{I}}/\mathrm{Log}\ U$ et $\mathrm{Gal}(k_\infty \cap k'_\infty/k)$ ne sont pas indépendants ; ceci peut se faire en étudiant la suite

exacte de cohomologie déduite de la suite exacte de H-modules :

$$0 \longrightarrow \mathrm{Gal}(\tilde{k}/\tilde{H}_k) \longrightarrow \tilde{G} \longrightarrow \widetilde{Cl} \longrightarrow 0 .$$

On obtient alors le résultat suivant, toujours pour les corps quadratiques imaginaires et $p = 2$ .

PROPOSITION. - Sauf dans les cas où $C = \mathbb{Q}_2(\sqrt{-3})$ , $\mathbb{Q}_2(\sqrt{-14})$ , on a l'équivalence suivante :

Les $\mathbb{Z}_2$-extensions fondamentales $k_\infty$ et $k'_\infty$ de $k$ sont non linéairement disjointes sur $k$ (i. e. $\chi = 1$ ) si et seulement si le 2-corps de classes de Hilbert $H_k$ de $k$ et $\tilde{k}$ sont linéairement disjoints sur $k$ (i. e. $\overline{\mathrm{Log}\ I} = \mathrm{Log}\ U$ ).

Si $C = \mathbb{Q}_2(\sqrt{-3})$ , on a $\chi = 0$ (et $\tilde{H}_k = k$ ou non) ;

Si $C = \mathbb{Q}_2(\sqrt{-14})$ , on a $\tilde{H}_k \neq k$ (et $\chi = 0$ ou $1$ ).

Pour d'autres détails sur cette question, se reporter à [2].

(b) Lois de décomposition dans $\tilde{k}/k$ . - Soit $\mathfrak{q}$ un idéal premier de $k$ ; on entend par loi de décomposition de $\mathfrak{q}$ dans $\tilde{k}/k$ la connaissance du groupe de décomposition $\tilde{G}_\mathfrak{q}$ et celle du groupe d'inertie $\tilde{G}^0_\mathfrak{q}$ (et éventuellement des groupes de ramification supérieure $\tilde{G}^i_\mathfrak{q}$ , $i \geqslant 1$ ). On sait aussi que tout ceci est équivalent à la connaissance du symbole de reste normique de Hasse :

$$\left(\frac{a\ ,\ \tilde{k}/k}{\mathfrak{q}}\right) : k^\times \longrightarrow \tilde{G}_\mathfrak{q} ,$$

puisque l'image de $k^\times$ par ce symbole est dense dans $\tilde{G}_\mathfrak{q}$ , tandis que l'image du sous-groupe de $k^\times$ formé des éléments étrangers à $p$ est dense dans $\tilde{G}^0_\mathfrak{q}$ . Autrement dit, si l'on identifie $\tilde{G}$ à $\overline{\mathrm{Log}\ I}$ , on est ramené à calculer

$$\mathrm{Log}\left(\frac{a\ ,\ \tilde{k}/k}{\mathfrak{q}}\right) , \quad a \in k^\times .$$

Le résultat est le suivant.

Si $\mathfrak{q} = \mathfrak{l} \notin S$ (cas modéré), on a

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

où $v_\mathfrak{l}$ est la valuation $\mathfrak{l}$-adique ;

Si $\mathfrak{q} = \mathfrak{p} \in S$ (cas sauvage), on a

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

où $\log_\mathfrak{p}$ désigne maintenant le logarithme d'Iwasawa et Log l'extension correspondante obtenue comme au § 1.

On en déduit respectivement :

$$\tilde{G}_\mathfrak{l} = \mathbb{Z}_p\ \mathrm{Log}\ \mathfrak{l} ,$$

$\tilde{G}_{\mathfrak{p}} = ((\log_{\mathfrak{p}} \pi_{\mathfrak{p}} , 0 , \ldots , 0) - \mathrm{Log}\ \mathfrak{p})\ \underset{\sim}{Z}_p + \log_{\mathfrak{p}} U_{\mathfrak{p}} \times \{0\} \times \ldots \times \{0\}$ modulo $\underset{\sim}{Q}_p \log E$,

où $\pi_{\mathfrak{p}}$ est une uniformisante dans $k_{\mathfrak{p}}$.

On voit sur cette expression l'aspect local-global, $\log_{\mathfrak{p}} \pi_{\mathfrak{p}}$ étant l'aspect local, tandis que $\mathrm{Log}\ \mathfrak{p}$ n'est pas local (le résultat est lié à l'ordre de la classe de $\mathfrak{p}$ dans Cl ).

Le cas des groupes d'inertie est très simple ; on a :

$$\tilde{G}^0_{\mathfrak{p}} = \tilde{G}^1_{\mathfrak{p}} = (\log_{\mathfrak{p}} U_{\mathfrak{p}}) \times \{0\} \times \ldots \times \{0\} \quad \text{modulo} \quad \underset{\sim}{Q}_p \log E .$$

Exemple. - Considérons $k = \underset{\sim}{Q}(\sqrt{-15})$ et $p = 2$. On a $S = \{\mathfrak{p} , \bar{\mathfrak{p}}\}$ car 2 est décomposé. On a $Cl \simeq \underset{\sim}{Z}/2\ \underset{\sim}{Z}$, et le calcul de $\overline{\mathrm{Log}\ I}$ conduit à

$$\tilde{G} = (2 , 2)\ \underset{\sim}{Z}_2 \oplus (4 , 0)\ \underset{\sim}{Z}_2 .$$

Calculons $\tilde{G}_{\mathfrak{p}}$ ; on a $\pi_{\mathfrak{p}} = 2$ (donc $\log_{\mathfrak{p}} \pi_{\mathfrak{p}} = 0$ ) et, $\mathfrak{p}$ n'étant pas principal, on calcule son carré :

$$\mathfrak{p}^2 = \left(\frac{1 + \sqrt{-15}}{2}\right) ;$$

d'où $\mathrm{Log}\ \mathfrak{p} = 1/2\ \mathrm{Log}\left(\frac{1 + \sqrt{-15}}{2}\right) \equiv (2 , 2)$ modulo $(4 , 4)$ ; ce qui donne immédiatement :

$$\tilde{G}_{\mathfrak{p}} = (2 , 2)\ \underset{\sim}{Z}_2 \oplus (4 , 0)\ \underset{\sim}{Z}_2 \ (= \tilde{G} \text{ ici}).$$

## BIBLIOGRAPHIE


[1] GRAS (Georges). - Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres, J. für reine und angew. Math., t. 333, 1982, p. 86-132.

[2] GRAS (Georges). - Sur les $\underset{\sim}{Z}_2$-extensions d'un corps quadratique imaginaire, Ann. Inst. Fourier, Grenoble, t. 33, 1983, fasc. 4, p. 1-18.

[3] GRAS (Georges). - Decomposition and inertia groups in $\underset{\sim}{Z}_p$-extensions (à paraitre).

[4] GRAS (Georges). - Plongements kummériens dans les $\underset{\sim}{Z}_p$-extensions, Compos. Math., Groningen (à paraître).

[5] GRAS (Georges). - Remarks on $K_2$ of number fields, J. of number Theory (à paraître).