

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 de travail d'analyse ultramétrique
(Secrétariat mathématique, Paris), 1983-1984, tous droits réservés.

L'accès aux archives de la collection « Groupe de travail d'analyse ultramétrique » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

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 $S = \{\text{idéaux premiers } \mathfrak{p} \text{ de } k \text{ divisant } p\}$; 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),

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

$\text{Log} : U \rightarrow B = C/\mathbb{Q}_p \log E$ (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 ;

$$\begin{array}{ccccccc} & & T' & \xrightarrow{\quad} & T & & \\ & & \downarrow & & \downarrow & & \\ 1 & \xrightarrow{\quad} & U/\bar{E} & \xrightarrow{\quad} & G & \xrightarrow{\quad} & Cl \xrightarrow{\quad} 1 \\ & & \downarrow \text{Log} & & \downarrow \log & & \\ 0 & \xrightarrow{\quad} & \text{Log } U & \xrightarrow{\quad} & \text{Log } G & & \end{array}$$

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. $\text{Log} = \log$ 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.

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \\
 1 & \dashrightarrow & U & \dashrightarrow & G & \dashrightarrow & \mathbb{Z}/3\mathbb{Z} \dashrightarrow 0 \\
 & & \downarrow \log & & \uparrow \exp & & \downarrow \log \\
 0 & \dashrightarrow & 3\mathbb{Z}_3 \oplus 3\sqrt{-1}\mathbb{Z}_3 & \dashrightarrow & 3\mathbb{Z}_3 \oplus \sqrt{-1}\mathbb{Z}_3 & \dashrightarrow & \mathbb{Z}/3\mathbb{Z} \dashrightarrow 0 \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
 \end{array}$$

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 $S = \{p | p \text{ dans } k\}$). Elle conduit au schéma galoisien suivant

$$\begin{array}{ccccc}
 & & T & & \\
 & & \text{---} & & \\
 & \tilde{k} & \text{---} & \tilde{k} & H_k & \text{---} & \hat{k} \\
 & | & & | & & & \\
 & \tilde{H}_k & \text{---} & H_k & & & \\
 & | & & | & & & \\
 & \mathbb{C}_1 & & \mathbb{C}_1 & & & \\
 & | & & | & & & \\
 & k & & k & & & \\
 & & \text{---} & & G & &
 \end{array}$$

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

Le groupe $\tilde{G} = \text{Gal}(\tilde{k}/k) \simeq G/T$ est isomorphe à $\mathbb{Z}_p^\gamma$, $\gamma \geq 1$ 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/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

$$\alpha : I \longrightarrow G$$

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

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 défini dans l'introduction les objets suivants :

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

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

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

on constate alors que Log est nul sur $\text{Ker } \alpha$ (car $\text{Ker } \alpha = \bigcap_{n \in \mathbb{N}} P_n$), 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 :

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

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 avons en vue

$$\tilde{G} \xrightarrow[\cong]{\text{Log}} \overline{\text{Log } I}.$$

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 $T = \text{Gal}(\hat{k}/\tilde{k})$ et $\tilde{Cl} = \text{Gal}(\tilde{H}_k/k)$ principalement).

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

COROLLAIRE 2. - On a $|T| = (|Cl| / (\overline{\text{Log } I} : \text{Log } U)) |T'|$ (où $|T'| = |\text{tor}(U/\bar{E})|$ 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 $\overline{\text{Log } I}$).

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

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

On a

$$\begin{aligned} \text{Log } I_{13} &= \frac{1}{3} \text{Log}(21 + 2\sqrt{-439}) = \frac{1}{6} \text{Log}(21 + 2\sqrt{-439})^2 \\ &= \frac{1}{6} \text{Log}(-1 - 1314 + 84\sqrt{-439}) \equiv \sqrt{-439} \pmod{3} = \text{Log } U, \end{aligned}$$

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

Dans ce cas on obtient :

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

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

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

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

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

(iii) Plongement kummérien dans $\widetilde{k}$: Si le groupe μ_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 $\widetilde{R}$ de $k^\times$ tel que $k(\sqrt[p]{R}) \subset \widetilde{k}$ (i. e. le radical de l'extension de k maximale d'exposant p contenue dans $\widetilde{k}$) ;

(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 $\mathbb{Q}(\frac{\mu}{p})$, 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

$$H = \{1, s\} = \text{Gal}(k/Q).$$

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

k_∞ , la $\mathbb{Z}_2$ -extension cyclotomique de k ,

k'_∞ , la $\mathbb{Z}_2$ -extension de k prodiédrale sur Q .

On démontre facilement que k_∞ est fixe par

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

que k'_∞ est fixe par

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

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

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

Plus précisément, on a le résultat suivant.

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

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

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

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

Le calcul de χ est alors standard en utilisant Log ; on a :

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

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

$$\overline{\text{Log } \tilde{I}} = 2 \mathbb{Z}_2 \oplus \sqrt{-82} \mathbb{Z}_2,$$

d'où $\overline{\text{Log } \tilde{I}^H} = 2 \mathbb{Z}_2$, d'où $\chi = 0$.

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

$$\overline{\text{Log } \tilde{I}} = 4 \mathbb{Z}_2 \oplus (2 + \sqrt{-34}) \mathbb{Z}_2,$$

ce qui donne

$$\overline{\text{Log } \tilde{I}^H} = 4 \mathbb{Z}_2 \text{ et } \chi = 1.$$

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

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

$$0 \longrightarrow \text{Gal}(\tilde{K}/\tilde{H}_k) \longrightarrow \tilde{G} \longrightarrow \tilde{Cl} \longrightarrow 0 .$$

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_∞ et k'_∞ de k sont non linéairement disjointes sur $\cdot k$ (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. $\overline{\text{Log } I} = \text{Log } U$).

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

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

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

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

Le résultat est le suivant.

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

$$\text{Log} \left(\frac{a, \tilde{k}/k}{l} \right) = -v_l(a) \text{Log } l ,$$

où v_l est la valuation l -adique ;

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

$$\text{Log} \left(\frac{a, \tilde{k}/k}{p} \right) = (\log_p a, 0, \dots, 0) - v_p(a) \text{Log } p ,$$

où $\log_p$ désigne maintenant le logarithme d'Iwasawa et Log l'extension correspondante obtenue comme au § 1.

On en déduit respectivement :

$$\tilde{G}_l = \mathbb{Z}_p \text{Log } l ,$$

$$\tilde{G}_\varphi = ((\log_\varphi \pi_\varphi, 0, \dots, 0) - \text{Log } \varphi) \mathbb{Z}_p + \log_\varphi U_\varphi \times \{0\} \times \dots \times \{0\} \text{ modulo } \mathbb{Q}_p \log E,$$

où π_φ est une uniformisante dans k_φ .

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

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

$$\tilde{G}_\varphi^0 = \tilde{G}_\varphi^1 = (\log_\varphi U_\varphi) \times \{0\} \times \dots \times \{0\} \text{ modulo } \mathbb{Q}_p \log E.$$

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

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

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

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

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

$$\tilde{G}_\varphi = (2, 2) \mathbb{Z}_2 \oplus (4, 0) \mathbb{Z}_2 (= \tilde{G} \text{ ici}).$$

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 $\mathbb{Z}_2$ -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 $\mathbb{Z}_p$ -extensions (à paraître).
- [4] GRAS (Georges). - Plongements kummériens dans les $\mathbb{Z}_p$ -extensions, Compos. Math., Groningen (à paraître).
- [5] GRAS (Georges). - Remarks on K_2 of number fields, J. of number Theory (à paraître).