Groupe de travail
d'analyse ultramétrique

Thong Nguyen-Quang-Do

Formulations algébriques de la conjecture de Leopoldt et applications

Groupe de travail d'analyse ultramétrique, tome 9, n° 2 (1981-1982), exp. n° 19, p. 1-6
<http://www.numdam.org/item?id=GAU_1981-1982__9_2_A2_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
9e année, 1981/82, n° 19, 6 p.

15 mars 1982

FORMULATIONS ALGÉBRIQUES DE LA CONJECTURE DE LEOPOLDT ET APPLICATIONS

par NGUYEN-QUANG-DO Thong (*)

Soient k un corps de nombres, et p un nombre premier fixé. Le but de cet exposé est de donner (sans prétendre être exhaustif) diverses formulations algébriques de la conjecture de Leopoldt pour k et p, avec, pour chaque formulation, des applications en direction de la démonstration de cette conjecture.

On notera toujours r_1 et r_2 les nombres respectifs de places réelles et complexes de k, et $\rho = r_1 + r_2 - 1$ le $\mathbb{Z}$-rang du groupe des unités E_k de k.

1. Rappels.

Soit (u_i) un système fondamental d'unités de k. On pose la matrice

$$R_p = (\log_p \iota(u_i)) ,$$

où $\log_p$ désigne le logarithme p-adique, et ι parcourt les plongements de k dans Ω_p (= complété de $\bar{\mathbb{Q}}_p$).

CONJECTURE DE LEOPOLDT. - *Le rang de la matrice R_p est maximal, c'est-à-dire égal à ρ*

Si le corps k est totalement réel, cette conjecture équivaut à $\det R_p \neq 0$, c'est-à-dire à la non-nullité du régulateur p-adique [7].

Par des méthodes "à la Baker", A. BRUMER a démontré le théorème suivant.

THÉORÈME 1 (BRUMER [1]). - *Si k est une extension abélienne de $\mathbb{Q}$ ou d'un corps quadratique imaginaire, k vérifie la conjecture de Leopoldt.*

Pour d'autres résultats de type analytique, voir par exemple l'exposé d'EMSALEM [3]

2. Traduction par le corps de classes.

Il est immédiat que le rang de R_p ne change pas si l'on prend, à la place des u_i, des éléments de E_k engendrant un sous-groupe de E_k d'indice fini. On prend d'habitude le sous-groupe E_k^1, défini comme suit.

(*) Texte reçu le 4 octobre 1982.
NGUYEN-QUANG-DO Thong, 49 rue Pierre Valette, 92240 MALAKOFF.

Pour toute place v de k au-dessus de p, soit U_v^1 le groupe des unités principales du complété k_v de k. Soit $U^1 = \prod_{v/p} U_v^1$. Posons

$$E_k^1 = \{x \in E_k \ ; \ i(x) \in U^1\} ,$$

où i désigne le plongement diagonal. Désignons par $\overline{i(E_k^1)}$ la fermeture de $i(E_k^1)$ pour la topologie-produit. Par le corps de classes, nous avons une suite exacte :

$$(*) \qquad 0 \longrightarrow U^1/\overline{i(E_k^1)} \longrightarrow \mathrm{Gal}(M_k/F_k) \longrightarrow A_k \longrightarrow 0 ,$$

où : F_k = p-extension abélienne maximale non ramifiée de k,

M_k = p-extension abélienne maximale non ramifiée en toute place de k ne divisant pas p,

A_k = p-groupe des classes d'idéaux de k.

Posons enfin $\delta(k) = \mathrm{rang}_{\mathbb{Z}_p} \mathrm{Ker}(E_k^1 \otimes \mathbb{Z}_p \longrightarrow \overline{i(E_k^1)})$ (cet homomorphisme envoie $u_j \otimes a_j$ sur $i(u_j)^{a_j}$; il est surjectif).

THÉORÈME 2. - Les conditions suivantes sont équivalentes :

(i) k vérifie la conjecture de Leopoldt,

(ii) $\mathrm{rang}_{\mathbb{Z}_p} X_k = 1 + r_2$, où $X_k = \mathrm{Gal}(M_k/k)$,

(iii) $\delta(k) = 0$ ($\delta(k)$ est appelé le "défaut" de la conjecture de Leopoldt).

Preuve. - En prenant les $\mathbb{Z}_p$-rangs dans la suite exacte (*), on a :

$$\mathrm{rang}_{\mathbb{Z}_p} X_k = \mathrm{rang}_{\mathbb{Z}_p} U_k^1 - \mathrm{rang}_{\mathbb{Z}_p} \overline{i(E_k^1)} = r_1 + 2r_2 - \rho + \delta(k) = 1 + r_2 + \delta(k) .$$

Q. E. D.

Une autre façon d'exprimer la condition (ii) est de dire que k doit posséder exactement $(1 + r_2)$ $\mathbb{Z}_p$-extensions indépendantes.

Remarque 1. - Au lieu de considérer seulement les places de k divisant p, on peut introduire un ensemble fini S de places de k, contenant toutes les places divisant p. En désignant alors par M_k la p-extension abélienne maximale de k non ramifiée hors de S, et $X_k = \mathrm{Gal}(M_k/k)$, le théorème 2 reste entièrement valable.

Application. - Supposons maintenant que k contient le groupe μ_p des racines p-ièmes de l'unité. Suivant BERTRANDIAS et PAYAN [2], introduisons les deux sous-groupes suivants de $k^\times/k^{\times p}$:

$\Phi_k = \{a \in k^\times/k^{\times p}$; $k(\sqrt[p]{a})$ se plonge dans une $\mathbb{Z}_p$-extension de $k\}$,

$\Psi_k = \{a \in k^\times/k^{\times p}$; $k(\sqrt[p]{a})$ se plonge, pour tout entier n , dans une surextension cyclique de k , de degré égal à $p^n\}$.

En notant dim la dimension sur le corps $\mathbb{F}_p$, il est clair que $\dim \Psi_k \geq \dim \Phi_k$ (pas d'égalité en général), et $\dim \Phi_k \geq 1 + r_2$, avec égalité si, et seulement si, k vérifie la conjecture de Leopoldt (voir théorème 2). Pour que k vérifie Leopoldt il suffit donc que $\dim \Psi_k = 1 + r_2$.

Exemples ([2], [8]).

(i) $p = 3$, $k = \mathbb{Q}(\sqrt{-3}, \sqrt{d})$.
Pour $d = -2, -5, -11, -14, -17, -35$, $\dim \Psi_k = 1 + r_2 = 3$.
Pour $d = 83$, $\dim \Psi_k = 4$.

(ii) $p = 5$, $k = \mathbb{Q}(\sqrt{-11}, \mu_p)$, alors $\dim \Psi_k = 2 + r_2$.

(iii) $k = \mathbb{Q}(\mu_p)$, p irrégulier, alors $\dim \Psi_k > 1 + r_2$.

(iv) $p = 3$, $k = \mathbb{Q}(\sqrt{-1}, \sqrt{7}, \sqrt[4]{\alpha})$, avec $\alpha = -3(2 + \sqrt{7})^2$. On vérifie que $k = \mathbb{Q}(\sqrt{7}).N$, où $N = \mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{6 + 4\sqrt{-3}})$ (corps diédral), et $\dim \Psi_k = 1 + r_2$.

THÉORÈME 3 (MIKI [8]). - Les conditions suivantes sont équivalentes :

(i) $\dim \Psi_k = 1 + r_2$.

(ii) $X_k \simeq \mathbb{Z}_p^{1+r_2} \times (\prod_{v/p} \mu_{k_v})/\mu_k$, où μ_L désigne le p-groupe des racines de l'unité contenues dans le corps L .

Exemple. - $p = 3$, $k = \mathbb{Q}(\sqrt[3]{(2 + 3\sqrt{-3})(4 + 3\sqrt{-3})}, \mu_p)$. Alors $X_k \simeq (\mathbb{Z}/3)^2 \times (\mathbb{Z}_3)^3$.

3. Traduction par la théorie d'Iwasawa.

Dans toute cette section, k_∞/k désigne la $\mathbb{Z}_p$-extension cyclotomique de k , $\Gamma = \mathrm{Gal}(k_\infty/k)$, $\Lambda = \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]]$ (l'algèbre d'Iwasawa des séries formelles en T , à coefficients dans $\mathbb{Z}_p$). Deux modules d'Iwasawa vont intervenir de façon essentielle :

M_∞ = la p-extension abélienne maximale de k_∞ , non ramifiée en toute place de k_∞ ne divisant pas p , et $X_\infty = \mathrm{Gal}(M_\infty/k_\infty)$.

L_∞ = la p-extension abélienne maximale de k_∞ , non ramifiée, décomposant totalement toute place de k_∞ divisant p , et $Y_\infty = \mathrm{Gal}(L_\infty/k_\infty)$.

X_∞ et Y_∞ sont des Λ-modules, via l'action naturelle de Γ .

On peut maintenant compléter le théorème 3.

THÉORÈME 4 (GILLARD [4]). - Si $\dim \psi_k = 1 + r_2$, alors $Y_\infty = 0$. La réciproque est vraie si aucune place de k au-dessus de p ne se décompose dans k_∞/k.

Les modules Y_∞ et X_∞ sont liés par un résultat fondamental d'IWASAWA [6].

Soit N_∞ l'extension de k_∞ obtenue en ajoutant toutes les racines p^n-ièmes (n variable) des p-unités de k_∞. Alors $\mathrm{Gal}(M_\infty/N_\infty)$ est quasi isomorphe à $\dot{Y}_\infty$, où la notation (.) signifie qu'on a "tordu" le module Y_∞ par le caractère cyclotomique. Le module X_∞ lui-même vérifie le théorème suivant.

THÉORÈME 5 (IWASAWA [6]). - On a $\mathrm{rang}_\Lambda X_\infty = r_2$.

COROLLAIRE 1. - On a $\delta(k) = \mathrm{rang}_{Z_p} X_\infty^\Gamma = \mathrm{rang}_{Z_p} \dot{Y}_\infty^\Gamma$. En particulier, k vérifie la conjecture de Leopoldt si, et seulement si, $X_\infty^\Gamma = 0$, si, et seulement si, $\dot{Y}_\infty^\Gamma = 0$.

Preuve. - D'après le théorème de structure pour les Λ-modules, on a :

$$\mathrm{rang}_{Z_p} X_\infty/TX_\infty = r_2 + \mathrm{rang}_{Z_p} X_\infty^\Gamma .$$

Or la théorie de Galois fournit une suite exacte

$$0 \longrightarrow X_\infty/TX_\infty \longrightarrow X_k \longrightarrow Z_p \longrightarrow 0 .$$

Q. E. D.

COROLLAIRE 2. - Soit (k_n) la tour canonique des extensions cycliques contenues dans k_∞/k. Alors les défauts $\delta(k_n)$ sont bornés ("forme faible" de Leopoldt, voir [5]).

Preuve. - Comme précédemment, $\delta(k_n) = \mathrm{rang}_{Z_p} X_\infty^{\Gamma_n}$, où $\Gamma_n = \mathrm{Gal}(k_\infty/k_n)$. Or X_∞ est un Λ-module noethérien, donc la suite des sous-modules $X_\infty^{\Gamma_n}$ est stationnaire.

Q. E. D.

Remarque 2. - IWASAWA [6] a montré que X_∞ n'a pas de sous-module fini non nul. La condition $X_\infty^\Gamma = 0$ équivaut à ce que T ne divise pas la série caractéristique de X_∞.

4. Traduction par la cohomologie galoisienne.

Les notations sont les mêmes que dans la section 2. En outre, désignons par G_k le groupe de Galois de la p-extension (non abélienne) maximale de k, non ramifiée en toute place de k ne divisant pas p. Soit d (resp. r) le nombre minimal de générateurs (resp. de relations) du groupe G_k. Par définition, on a

$$d = \dim H^1(G_k , F_p) \quad \text{et} \quad r = \dim H^2(G_k , F_p) ,$$

et l'on sait que $-1 + d - 2 = r_2$ (caractéristique d'Euler-Poincaré). Par des considérations de suites spectrales, on montre le théorème suivant.

THÉORÈME 6 (voir [9]). - Soit K une extension galoisienne finie de k, non ramifiée hors de p, dont le groupe de Galois est un p-groupe G. On a une suite exacte de $(\mathbb{Z}_p\, G)$-modules.

$$(**) \qquad 0 \longrightarrow \Delta(K) \longrightarrow (\mathbb{Z}_p\, G)^r \longrightarrow R_d^{ab}(G) \longrightarrow X_K \longrightarrow 0\ ,$$

où $\Delta(K)$ est le dual de Pontrjagin de $H^2(G_K\ ,\ \mathbb{Q}_p/\mathbb{Z}_p)$, et le module $R_d^{ab}(G)$ est le "module des relations" de G, défini comme suit.

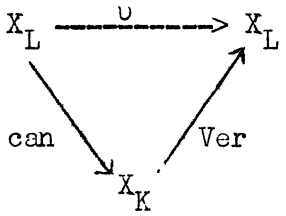
Considérons G comme un quotient du pro-p-groupe libre F_d à d générateurs. Soit R_d le noyau de la projection $F_d \longrightarrow G$. Par définition, $R_d^{ab}(G)$ est l'abélianisé de R_d, sur lequel G opère naturellement.

COROLLAIRE. - On a $\delta(K) = \operatorname{rang}_{\mathbb{Z}_p} \Delta(K)$. En particulier, K vérifie la conjecture de Leopoldt si, et seulement si, $H^2(G_K\ ,\ \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

Preuve. - Il suffit de calculer les $\mathbb{Z}_p$-rangs dans la suite exacte (**), en sachant que $\operatorname{rang}_{\mathbb{Z}_p} R_d^{ab}(G) = \#\, G(d-1) + 1$.

Q. E. D.

Propriété fonctorielle. - Soit L/k une surextension contenant K/k. On a un diagramme commutatif :



où can est l'homomorphisme canonique $G_L^{ab} \longrightarrow G_K^{ab}$, Ver est le transfert $G_K^{ab} \longrightarrow G_L^{ab}$, et υ est la norme $\sum_{\sigma \in E} \sigma$, $E = \operatorname{Gal}(L/k)$.

THÉORÈME 7. - On garde les hypothèses du théorème 6. Si k vérifie la conjecture de Leopoldt, alors K la vérifie également.

Preuve. - D'après le théorème 6 et la propriété fonctorielle, on a un diagramme commutatif aux lignes exactes :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Delta(K) & \longrightarrow & (\mathbb{Z}_p\, G)^r & \longrightarrow & R_d^{ab}(G) & \longrightarrow & X_K \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \Delta(k) & \longrightarrow & (\mathbb{Z}_p)^r & \longrightarrow & R_d^{ab}(1) = (\mathbb{Z}_p)^d & \longrightarrow & X_k \longrightarrow 0
\end{array}$$

où les flèches verticales sont les flèches canoniques.

On en déduit deux diagrammes commutatifs :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta(K) & \longrightarrow & (\mathbb{Z}_p\ G)^r & \longrightarrow & T_K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Delta(k) & \longrightarrow & (\mathbb{Z}_p)^r & \longrightarrow & T_k & \longrightarrow & 0 \end{array} \qquad \text{et} \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & T_K & \longrightarrow & R_d^{ab}(G) & \longrightarrow & X_K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T_k & \longrightarrow & (\mathbb{Z}_p)^d & \longrightarrow & X_k & \longrightarrow & 0 \end{array}$$

De plus, par définition du module des relations, on sait que le transfert $R_d^{ab}(1) \longrightarrow R_d^{ab}(G)$ est injectif. Le lemme des cinq et la propriété fonctorielle montrent alors que $\upsilon(T_K) \simeq T_k$, où $\upsilon = \sum_{\sigma \in G} \sigma$.

Supposons que k vérifie Leopoldt. Alors $T_k \simeq (\mathbb{Z}_p)^r$, d'où $\upsilon(T_K) \simeq (\mathbb{Z}_p)^r$, d'où $\upsilon(T_K/p\ T_K) \simeq (\mathbb{F}_p)^r$. Comme T_K est sans torsion (en tant que sous-groupe de R_d^{ab}), il résulte d'un lemme de représentation modulaire bien connu que le $(\mathbb{Z}_p\ G)$-module T_K admet $(\mathbb{Z}_p\ G)^r$ comme facteur direct. Un calcul de $\mathbb{Z}_p$-rangs dans la suite exacte (**) montre alors que $\text{rang}_{\mathbb{Z}_p} X_K \leqslant 1 + \#|G|\ r_2$, i. e. K vérifie Leopoldt.

Q. E. D.

BIBLIOGRAPHIE

[1] BRUMER (A.). - On units of algebraic number fields, Mathematika, London, t. 14, 1967, p. 121-124.

[2] BERTRANDIAS (F.) et PAYAN (J.-J.). - Γ-extensions et invariants cyclotomiques, Ann. scient. Ec. Norm. Sup., 4e série, t. 5, 1972, p. 517-543.

[3] EMSALEM (M.). - Comportement des fonctions L p-adiques au voisinage de zéro, Groupe d'étude d'Analyse ultramétrique, 9e année, 1981/82, n° 17, 19 p.

[4] GILLARD (R.). - Formulations de la conjecture de Leopoldt et étude d'une condition suffisante, Abh. Seminar Univ. Hamburg, t. 48, 1979, p. 125-138.

[5] GREENBERG (R.). - On the structure of certain Galois groups, Invent. Math., Berlin, t. 47, 1978, p. 85-99.

[6] IWASAWA (K.). - On $\mathbb{Z}_p$-extensions of algebraic number fields, Annals of Math., Series 2, t. 98, 1973, p. 246-326.

[7] LEOPOLDT (H. W.). - Zur Arithmetik in abelschen Zahlkörpern, J. für reine und angew. Math., t. 209, 1962, p. 54-71.

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

[9] NGUYEN-QUANG-DO (T.). - Formations de classes et modules d'Iwasawa (à paraître).