

JEAN-JACQUES PAYAN

Contre-exemple d'Iwasawa à une conjecture d'Iwasawa

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 2, p. 1-9

http://www.numdam.org/item?id=STNG_1974-1975__4__A2_0

© Institut Fourier – Université de Grenoble, 1974-1975, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble 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/>

19 décembre 1974

Grenoble

 CONTRE-EXEMPLE D'IWASAWA A UNE CONJECTURE D'IWASAWA [2]

par Jean Jacques PAYAN

On appelle \mathbb{Z}_ℓ -extension d'un corps de nombres k une extension galoisienne infinie K telle que $\Gamma = \text{Gal } K/k$ soit isomorphe à \mathbb{Z}_ℓ . On note k_n l'extension intermédiaire de degré ℓ^n sur k . k_n/\mathbb{Q} étant finie, le groupe \mathfrak{H}_n des classes d'idéaux de k_n est fini, on note e_n la plus haute puissance de k qui divise $\text{Card } \mathfrak{H}_n$. Iwasawa a prouvé, en utilisant la structure du $\mathbb{Z}[\Gamma]$ -module $\varprojlim \mathfrak{H}_n$, que pour n suffisamment grand e_n vérifie

$$e_n = \lambda_n + \mu \ell^n + \nu \quad \text{où } \lambda, \mu, \nu$$

sont des constantes qui ne dépendent que du corps K . [1], [3]. On pose $\lambda = \lambda(K/k)$, $\mu = \mu(K/k)$.

K/k désignant toujours une \mathbb{Z}_ℓ -extension, on note M la ℓ -extension abélienne non ramifiée maximale de K , $\text{Gal } M/K$ est alors muni d'une structure de \mathbb{Z}_ℓ -module et on montre [3] que $\mu(K/k) = 0$ signifie que $\text{Gal } M/K$ est de type fini sur \mathbb{Z}_ℓ . Cela équivaut encore à la propriété suivante : le ℓ -rang de \mathfrak{H}_n , c'est-à-dire la dimension sur F_ℓ de $\mathfrak{H}_n \otimes F_\ell$, est borné.

Après avoir étudié quelques cas particuliers et donné des exemples numériques Iwasawa a conjecturé que $\mu(K/k) = 0$. On va exposer dans ce qui suit comment Iwasawa a prouvé la fausseté de cette conjecture en même temps qu'il montrait que $\mu(K/k) = 0$ pour une vaste classe de

\mathbb{Z}_ℓ -extensions.

I. CONSEQUENCES DE LA DECOMPOSITION.

Soit K/k une \mathbb{Z}_ℓ -extension, k corps de nombres. Soit Z_p le groupe de décomposition dans K/k d'un idéal premier p de k , Z_p est la limite projective des groupes de décomposition de p dans les k_n/k , c'est donc un sous-groupe fermé de Γ , il est donc soit réduit à l'identité, soit égal à un sous-groupe d'indice fini. Le nombre g_n d'idéaux premiers de k_n au-dessus de p est donc ou bien égal à ℓ^n , pour tout n , ou bien borné. Dans la première éventualité, on dit que p est complètement décomposé.

Supposons que k contient le groupe μ_ℓ des racines ℓ -ièmes de l'unité et qu'il existe t , $t \geq 1$, idéaux premiers p_1, \dots, p_t de k complètement décomposés dans K/k . Choisissons $\alpha \in k^*$ tel que l'idéal (α) vérifie $(\alpha) = p_1 \dots p_t^m$ où m est premier avec les p_i et posons $k' = k(\sqrt[\ell]{\alpha})$, $K' = Kk'$. Comme k'/k est ramifiée en $p_1 \dots p_t$, $k' \cap K = k$ et K'/k' est une \mathbb{Z}_ℓ -extension. Pour $n \geq 0$, on note $k'_n = k' \circ k_n = k_n(\sqrt[\ell]{\alpha})$, k'_n/k_n est donc cyclique de degré ℓ , notons $\ell^{e'_n}$ la plus haute puissance de ℓ qui divise le nombre de classes de k'_n . Alors pour n suffisamment grand $e'_n = \lambda'_n + \mu' \ell^n + \nu'$ avec $\lambda' = \lambda(K'/k')$, $\mu' = \mu(K'/k')$.

Soit s_n le nombre de diviseurs premiers de k_n ramifiés dans k'_n . Chaque p_i ayant ℓ^n diviseurs premiers dans k_n et ceux-ci étant ramifiés dans k'_n on obtient :

$$t\ell^n \leq s_n.$$

Soient alors \mathfrak{H}'_n le groupe des classes de k'_n et σ un générateur de k'_n/k_n . La formule des classes ambiges s'écrit

$$[\mathfrak{H}'_n : \mathfrak{H}'_n^{1-\sigma}] = \frac{h'_n \cdot \ell^{s_n-1}}{[E'_n : E^*_n]}$$

où h_n , E_n , E_n^* ont des significations évidentes. On pose $d = [k:\mathbb{Q}]$, $d_n = [k_n:\mathbb{Q}] = \ell^{nd}$. E_n est abélien à $\frac{d_n}{2}$ générateurs au plus, de $E_n^\ell \subset E_n^*$ résulte que $[E_n:E_n^*]$ divise $\ell^{d_n/2}$, le membre de gauche divise $h'_n = \text{Card } \mathfrak{H}'_n$ et on en déduit

$$e'_n \geq e_n + s_n - 1 - \frac{d_n}{2} \quad (e_n \geq 0)$$

d'où $e'_n \geq (t - \frac{d}{2})\ell^{n-1}$ et la comparaison des formules donnant e'_n et e_n pour n assez grand entraîne $\mu(K'/k') \geq t - \frac{d}{2}$.

II. MISE EN EVIDENCE D'UN CONTRE-EXEMPLE.

On prend $k = \mathbb{Q}^{(\ell)}$ si $\ell > 2$ et $k = \mathbb{Q}^{(4)} = \mathbb{Q}(\sqrt{-1})$ si $\ell = 2$, si bien que $[k:\mathbb{Q}] = d = \ell - 1$ ou 2 suivant que $\ell > 2$ ou $\ell = 2$. On pose $(\ell) = I^d$ et on note k_I le complété de k pour sa valuation I -adique, k_I est une extension de \mathbb{Q}_ℓ vérifiant : $k_I = k \cdot \mathbb{Q}_\ell$, $k \cap \mathbb{Q}_\ell = \mathbb{Q}$ donc $\text{Gal } k_I/\mathbb{Q}_\ell$ est canoniquement isomorphe à $\text{Gal } k/\mathbb{Q}$. On note J le \mathbb{Q}_ℓ -automorphisme qui opère sur μ_ℓ par passage à l'inverse.

Le groupe U des unités de k_I est compact et abélien, $\text{Gal } k_I/\mathbb{Q}_\ell$ opère sur U , le logarithme ℓ -adique définit un isomorphisme d'un sous-groupe d'unités distinguées avec un sous-groupe additif des entiers I -adiques, isomorphisme qui commute avec l'action de $\text{Gal } k_I/\mathbb{Q}_\ell$. On en déduit l'existence d'un sous-groupe fermé V de U tel que $U^{1+J} \subset V \subset U$ et $U/V \simeq \mathbb{Z}_\ell$.

Notons E le groupe des unités de k , E_+ le sous-groupe des unités réelles. Alors

$$E_+^{1+J} = E_+^2 \subset E_+ \subset E \subset U$$

de plus E/E_+ et E/E_+^2 sont finis d'après le théorème de Dirichlet. On en déduit que EU^{1+J}/U^{1+J} qui est isomorphe à $E/U^{1+J} \cap E$ est fini. Si on note \bar{E} la fermeture de E dans U et si on remarque que U^{1+J} est fermé, la finitude de EU^{1+J}/U^{1+J} entraîne que EU^{1+J} est fermé. D'où $E \subset EU^{1+J} \subset V \subset U$ puisque $V \supset E$ (à cause de $U/V \simeq \mathbb{Z}_\ell$ et $U^{1+J} \subset V$), il en résulte $(U/V)^{1+J} = 1$. Notons alors L le corps

de classes de Hilbert de k et M l'extension abélienne maximale de k non ramifiée en dehors de χ . Il est clair que $\mathbb{Q} \subset k \subset L \subset M$ et L/\mathbb{Q} et M/\mathbb{Q} galoisiennes. $\text{Gal}(L/k)$ est isomorphe au groupe des classes d'idéaux de k et L/k est finie. Il existe, d'après la théorie du corps de classes, un isomorphisme canonique entre $\text{Gal } M/L$ et U/E . Comme M est globalement invariant par la conjugaison complexe, la restriction J_M de J à M appartient à $\text{Gal } M/\mathbb{Q}$ et $\text{Gal } M/L$ étant distingué dans $\text{Gal } M/\mathbb{Q}$ on fait opérer J sur $\text{Gal } M/L$ par $\sigma^J = J\sigma J^{-1}$ pour tout σ de $\text{Gal } M/L$. Avec l'action de J sur U/E déjà mentionnée l'isomorphisme de $\text{Gal } M/L$ sur U/E est un $\mathbb{Z}[J]$ -isomorphisme. Soit alors F le corps intermédiaire de M/L associé à V/\bar{E} par cet isomorphisme. De $U^{1+J} \subset V$, résulte $V^J = V$ si bien que $(\text{Gal } M/F)^J = \text{Gal } M/F$ et $F^J = F$, donc la restriction J_F de J à F opère sur $\text{Gal } F/L$ comme J_M sur $\text{Gal } M/L$ et $\text{Gal } F/L \simeq \mathbb{Z}_\ell$, $(\text{Gal } F/L)^{1+J} = 1$.

Notons alors K l'extension intermédiaire de F/k qui appartient au sous- \mathbb{Z}_ℓ -module de torsion de $\text{Gal } F/k$. On a évidemment $K^J = K$. Comme $\text{Gal } L/k$ est fini on a $\text{Gal } K/k \simeq \mathbb{Z}_\ell$ et $(\text{Gal } K/k)^{1+J} = 1$. Notons encore k_n l'extension intermédiaire de K/k de degré ℓ^n sur k et k_+ le sous-corps réel maximal de k , comme $K^J = K$, K/k_+ est galoisienne de même que k_n/k_+ pour tout n de \mathbb{N} .

Posons $G_n = \text{Gal } k_n/k_+$ et $H_n = \text{Gal } k_n/k$. G_n est produit semi-direct de $H_n \simeq \mathbb{Z}/\ell^n\mathbb{Z}$ et du sous-groupe $\{1, J_{k_n}\}$. De plus $(\text{Gal } K/k) = 1$ implique $H_n^{1+J_{k_n}} = 1$ c'est-à-dire $J_{k_n} \sigma J_{k_n}^{-1} = \sigma^{-1}$ pour tout σ de H_n . G_n est donc un groupe diédral d'ordre $2\ell^n$.

p_+ désignant un idéal premier de k_+ , inerte dans k et p l'idéal unique de k qui divise p_+ . p_+ est premier à ℓ , comme $k_+ \subset k \subset k_n \subset K \subset M$ on voit que p_+ est non ramifié dans k_n , soit alors p_n un idéal premier de k_n divisant p_+ et Z_n le groupe de décomposition de p_n dans l'extension k_n/k_+ . Puisque p_+ est non

ramifié dans k_n et non décomposé dans k , Z_n est un sous-groupe cyclique de G_n tel que $G_n = Z_n H_n$. G_n étant diédral, Z_n est d'ordre 2 et vérifie $Z_n \cap H_n = \{1\}$. Mais $Z_n \cap H_n$ est le groupe de décomposition de p_n pour k_n/k . Donc $Z_n \cap H_n = 1$ entraîne p est totalement décomposé dans k_n . Comme c'est valable pour tout $n \geq 0$, on voit que p est totalement décomposé dans K .

Les lois, bien connues, de décompositions dans les corps cyclotomiques et le théorème de la progression arithmétique montrent qu'il existe une infinité d'idéaux premiers p_+ de k_+ inertes dans k/k_+ . Il existe donc une infinité d'idéaux premiers de k totalement décomposés dans K .

Les résultats du §I permettent alors d'énoncer en prenant $N \geq t - \frac{d}{2}$.

THEOREME I. Soit k le corps des racines ℓ -ièmes (resp. 4-ièmes) de l'unité, pour tout entier $N \geq 1$, il existe une extension cyclique k'/k de degré ℓ et une \mathbb{Z}_ℓ -extension K'/k' telles que $\mu(K'/k') \geq N$.

Remarque : Si ℓ est régulier, $\mu(K/k) = 0$ pour la \mathbb{Z}_ℓ -extension construite ci-dessus.

III. COMPLEMENTS SUR LE LIEN ENTRE DECOMPOSITION ET NULLITE DE $\mu(K/k)$.

Les groupes considérés ici étant des ℓ -groupes abéliens, on entendra par rang d'un tel groupe son ℓ -rang.

LEMME 1. Soient A un ℓ -groupe abélien fini et G un groupe cyclique à ℓ^e éléments, de générateur σ alors on a l'inégalité

$$\text{rang } A \leq \ell^e \times \text{rang } A/A^{\sigma-1}.$$

Démonstration : On remarque que la puissance ℓ^e -ième de l'application linéaire définie par $\sigma-1$ sur $A \otimes_{\mathbb{F}_\ell} \mathbb{F}_\ell$ est nulle et que

$$\text{rang } A/A^{\sigma-1} \leq \text{rang } A^{\sigma-1}/A^{(\sigma-1)^2} \leq \dots$$

Soient alors k un corps de nombres, k'/k cyclique de degré ℓ et A et A' les ℓ -groupes de Sylow des groupes de classes d'idéaux de k et k' , posons $r = \text{rang } A$, $r' = \text{rang } A'$ et s nombre d'idéaux premiers de k ramifiés dans k' .

LEMME 2. $r-1 \leq r' \leq \ell(r+s)$.

Démonstration : Notons L et L' les ℓ -extensions abéliennes non ramifiées maximales de k et k' , la théorie du corps de classe entraîne $A \simeq \text{Gal } L/k$, $A' \simeq \text{Gal } L'/k'$. Il est clair que $L \subset L'$; soit M l'extension intermédiaire de L'/k abélienne sur k maximale, $k' \subset M \subset L'$ et on sait que M appartient au sous-groupe dérivé de $\text{Gal } L'/k$, ce qui s'exprime dans le cas particulier considéré par $\text{Gal } L'/M = (\text{Gal } L'/k')^{\sigma-1}$ (où on fait opérer σ par automorphismes intérieurs). De $\text{Gal } M/k' = (\text{Gal } L'/k')/(\text{Gal } L'/M)$ résulte $r' = \text{rang } \text{Gal } L'/k' \leq \ell\text{-rang } \text{Gal } M/k'$. Notons v_1, \dots, v_s les diviseurs premiers de k ramifiés dans k' et T_i le groupe d'inertie de v_i pour M/k , comme M/k' est non ramifiée, chaque T_i est un sous-groupe d'ordre ℓ dans $\text{Gal } M/k$ et aucun autre diviseur premier de k que les v_i n'est ramifié dans M/k . Comme L est l'extension maximale non ramifiée de k contenue dans M on a $\text{Gal } M/L = T_1 \dots T_s$ le produit n'étant pas nécessairement direct. On en déduit :

$$\begin{aligned} \text{rang } \text{Gal } M/k' &\leq \text{rang } \text{Gal } M/k \leq \text{rang } \text{Gal } L/k \\ &\text{rang } \text{Gal } M/L \leq r+s \end{aligned}$$

d'où compte tenu de $r' \leq \ell\text{-rang } \text{Gal } M/k'$,

$$r' \leq \ell(r+s).$$

Par ailleurs $\text{rang } \text{Gal } L/k \leq \text{rang } \text{Gal } M/k \leq \text{rang } \text{Gal } k'/k + \text{rang } \text{Gal } M/k' \leq 1 + \text{rang } \text{Gal } L'/k'$

soit $r \leq 1+r'$.

Enonçons maintenant le

THEOREME II. K/k \mathbb{Z}_ℓ -extensions, k corps de nombres, totallement imaginaire si $\ell = 2$, k'/k ℓ -extension galoisienne finie, on pose $K' = Kk'$ et on suppose que tout idéal de k ramifié dans k'/k n'est pas totallement décomposé dans k . Alors $\mu(K/k) = 0 \Leftrightarrow \mu(K'/k') = 0$.

Démonstration : Soit k'' intermédiaire de k'/k , posons $K'' = Kk''$ de sorte que $K' = K'' \cdot k'$. Les hypothèses entraînent que si un idéal premier de k'' est ramifié dans k' , il a un groupe de décomposition d'indice fini dans K''/k'' . Comme $\text{Gal } k'/k$ est un ℓ -groupe fini, donc résoluble, on se ramène par "dévissage" au cas cyclique de degré premier ℓ . Plaçons nous donc dans ce cas et notons encore k_n (resp k'_n) l'extension intermédiaire de K/k (resp. K'/k') de degré ℓ^n . De deux choses l'une ; ou bien $K \cap k' = k$ ou bien $K \cap k' = k_1$. Dans le second cas $K' = K$, et $k'_n = k_{n+1}$ pour tout n de \mathbb{N} et $\mu(K'/k') = \ell \mu(K/k)$ d'après la définition de μ et l'énoncé en découle. Regardons alors le cas $K \cap k' = k$, alors $k'_n = k_n k'$ et k'_n/k_n est cyclique de degré k . Soient A_n et A'_n les ℓ -groupes de Sylow des groupes de classes d'idéaux de k_n et k'_n . On pose $r_n = \text{rang } A_n$, $r'_n = \text{rang } A'_n$ et s_n nombre de diviseurs premiers de k_n ramifiés dans k'_n , la formule du lemme 2 entraîne $r_n - 1 \leq r'_n \leq \ell(r_n + s_n)$ pour tout n de \mathbb{N} . Si $\ell > 2$ aucune place archimédienne de k_n n'est ramifiée dans k'_n . Si $\ell = 2$, k est totallement imaginaire et k_n aussi, les places archimédiennes sont encore non ramifiées, s_n est donc le nombre des idéaux premiers de k_n ramifiés dans k'_n . Soit \mathfrak{p}_n un tel idéal de k_n , il divise un idéal \mathfrak{p} de k qui est ramifié dans k' puisque $k'_n = k'_n k_n$. Un tel \mathfrak{p} a un corps de décomposition dans K/k de degré fini sur k , le nombre de diviseurs premiers de \mathfrak{p} dans k_n est borné. Donc les s_n sont bornés pour $n \geq 0$ et on en déduit via les inégalités ci-dessus que r_n est borné si et seulement si c'est vrai pour r'_n . D'après un rappel fait au début $\mu(K/k)$ (resp. $\mu(K'/k')$) est nul si et seulement si les r_n (resp les r'_n) sont bornés d'où l'énoncé.

Iwasawa rappelle qu'il a prouvé dans [1] que si k est un corps de nombres, K/k une \mathbb{Z}_ℓ -extension, k'/k une extension finie et $K' = k'.K$ alors $\mu(K/k) \leq \mu(K'/k')$ et $\lambda(K/k) \leq \lambda(K'/k')$.

IV. CAS DE LA \mathbb{Z}_ℓ -EXTENSION CYCLOTOMIQUE.

En notant K° l'unique \mathbb{Z}_ℓ -extension de \mathbb{Q} , on sait que $\lambda(K^\circ/\mathbb{Q}) = \mu(K^\circ/\mathbb{Q}) = \nu(K^\circ/\mathbb{Q}) = 0$. Pour tout corps de nombres k , $K^\circ k/k$ est une \mathbb{Z}_ℓ -extension, on note $\lambda_\ell(k)$, $\mu_\ell(k)$, $\nu_\ell(k)$, ses invariants d'Iwasawa. On sait en outre que tout idéal premier de k un corps de décomposition de degré fini dans cette \mathbb{Z}_ℓ -extension. Le théorème 2 donne dans ce cas :

THEOREME 2'. Soient k un corps de nombres, supposé totalement imaginaire si $\ell = 2$, et k' une ℓ -extension galoisienne finie de k alors $\mu_\ell(k) = 0 \Leftrightarrow \mu_\ell(k') = 0$.

COROLLAIRE. Soit k une ℓ -extension galoisienne finie de \mathbb{Q} alors $\mu_\ell(k) = 0$.

Démonstration : Pour $\ell > 2$ cela résulte du théorème 2' et de la remarque $\mu_\ell(\mathbb{Q}) = 0$. Pour $\ell = 2$, on pose $k' = k(\sqrt{-1})$, $k'/\mathbb{Q}(\sqrt{-1})$ est une 2-extension galoisienne finie totalement imaginaire et $\mu(\mathbb{Q}(\sqrt{-1})) = 0$ d'où $\mu_2(k') = 0$ qui entraîne d'après ce qui a été rappelé à la fin du III $\mu_2(k) = 0$.

Pour conclure, Iwasawa conjecture que pour tout ℓ et tout k $\mu_\ell(k) = 0$ et souligne que la nullité de $\mu(K/k)$ dépend étroitement de l'existence d'idéaux premiers de k totalement décomposés dans K/k .

-:-:-:-

BIBLIOGRAPHIE

- [1] K. IWASAWA - "On Γ -extensions of algebraic number fields". Bull. Amer. Math Soc 65 (1959) pp. 183-226.
- [2] K. IWASAWA - "On the μ -invariants of \mathbb{Z}_p -extensions". Number theory, Algebraic Geometry and Commutative Algebra. Kinokumya Tokyo (1973) pp. 1-11.
- [3] J.P. SERRE - "Classes des corps cyclotomiques". Séminaire Bourbaki (1958) 174 pp. 1-11.

-:-:-:-