

ROLAND GILLARD

**Formulations de la conjecture de Leopoldt et étude
d'une condition suffisante**

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 4, p. 1-19

http://www.numdam.org/item?id=STNG_1974-1975__4__A4_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/>

9 janvier 1975

Grenoble

FORMULATIONS DE LA CONJECTURE DE LEOPOLDT
ET ETUDE D'UNE CONDITION SUFFISANTE

par Roland GILLARD

Au §I, nous allons donner diverses formulations de la conjecture de Leopoldt (cf [3]) au moyen de la théorie des \mathbb{Z}_ℓ -extensions (cf [6]). Ceci permet de mettre en évidence une condition portant sur un objet lié à la \mathbb{Z}_ℓ -extension cyclotomique du corps considéré, cette condition impliquant immédiatement la conjecture de Leopoldt pour le corps étudié (cf (12) ci-dessous).

Au §II, nous étudions une condition introduite dans [2] impliquant aussi la conjecture de Leopoldt. Nous montrons (théorème 4) que cette condition est équivalente à celle du I et en déduisons grâce au théorème 6 la valeur des invariants λ et μ introduits par Iwasawa (cf [6]) pour quelques corps.

Dans tout ce qui suit, nous désignerons par ℓ un nombre premier fixé et par k un corps de nombres de degré fini dont le nombre de plongements réels sera noté r_1 , celui des plongements imaginaires étant $2r_2$. Pour toute place v de k , on appellera k_v le complété de k correspondant.

I - FORMULATIONS DE LA CONJECTURE DE LEOPOLDT.I.1. Rappels sur la conjecture de Leopoldt.

Expliquons d'abord que nous appellerons \mathbb{Z} -rang (respectivement \mathbb{Z}_ℓ -rang) d'un \mathbb{Z} -module (respectivement d'un \mathbb{Z}_ℓ -module) de type fini le rang du quotient de ce module par son sous-module de torsion ; de même si G désigne un groupe abélien de type fini annihilé par ℓ , on notera $\dim G$ sa dimension en tant qu'espace vectoriel sur le corps fini à ℓ éléments.

Désignons par E le groupe des unités de k . Pour chaque place v de k au-dessus de ℓ , notons U_v^1 le groupe des unités distinguées de k_v . Soit E^1 le sous-groupe de E formé des éléments qui sont dans chaque U_v^1 . Notons \overline{E}^1 la fermeture de l'image de E^1 dans le groupe topologique produit $\prod_{v|\ell} U_v^1$.

Le \mathbb{Z} -rang de E^1 est $r_1 + r_2 - 1$; le \mathbb{Z}_ℓ -rang de \overline{E}^1 peut donc s'écrire $r_1 + r_2 - 1 - \delta$ avec δ dans \mathbb{N} .

La conjecture de Leopoldt (cf [3]) énonce la nullité de δ . Ainsi δ est le défaut de la conjecture de Leopoldt.

Le \mathbb{Z}_ℓ -rang de $\prod_{v|\ell} U_v^1$ est bien connu : c'est la somme des degrés des k_v pour v divisant ℓ c'est donc le degré de k , $r_1 + 2r_2$. Le \mathbb{Z}_ℓ -rang du quotient $\prod_{v|\ell} U_v^1 / \overline{E}^1$ est donc $r_2 + 1 + \delta$.

Soit L_O (respectivement M_O) la ℓ -extension abélienne maximale de k qui soit non ramifiée (respectivement qui soit non ramifiée pour les places premières à ℓ). Le \mathbb{Z}_ℓ -rang du groupe de Galois $G(M_O/L_O)$ est $r_2 + 1 + \delta$ puisque ce groupe est isomorphe au quotient $\prod_{v|\ell} U_v^1 / \overline{E}^1$. Le \mathbb{Z}_ℓ -rang du groupe de Galois $G(M_O/k)$ est donc aussi $r_2 + 1 + \delta$.

Soit \mathbb{K} le corps composé des \mathbb{Z}_ℓ -extensions de k (c'est-à-dire des extensions galoisiennes de k dont le groupe de Galois est isomorphe à \mathbb{Z}_ℓ ; ces extensions sont d'ailleurs non ramifiées pour les places premières à ℓ cf [6] théorème 1). \mathbb{K} est une sous-extension galoisienne

de M_O et le groupe de Galois $G(M_O/k)$ est fini ; on a donc :

$$G(k/k) \simeq \mathbb{Z}_\ell^{r_2+1+\delta} . \quad (1)$$

Ceci fournit la traduction classique de la conjecture de Leopoldt selon laquelle le corps k n'aurait que r_2+1 \mathbb{Z}_ℓ -extensions "indépendantes".

Pour chaque n , choisissons une racine primitive de l'unité d'ordre ℓ^n , notée ζ_n . Dans toute la suite, on supposera que ζ_1 appartient à k (et $\zeta_2 \in k$ pour $\ell = 2$).

Ceci conduit (cf [2]) à introduire le sous-groupe Θ_k de k^\times formé des éléments α de k^\times tels que le corps $k(\sqrt[\ell]{\alpha})$ soit inclus dans une \mathbb{Z}_ℓ -extension de k . La théorie de Kummer et la formule (1) donnent immédiatement :

$$\dim \Theta_k / k^{\times \ell} = r_2 + 1 + \delta . \quad (2)$$

Pour étudier la condition $\delta = 0$ l'article [2] remplace le groupe Θ_k par un groupe plus gros : la condition obtenue sera étudiée dans §II.

I.2. Traduction dans la théorie des \mathbb{Z}_ℓ -extensions.

Désignons par K la \mathbb{Z}_ℓ -extension cyclotomique $k(\zeta_1, \zeta_2, \dots, \zeta_n, \dots)$ de k ; son groupe de Galois, isomorphe à \mathbb{Z}_ℓ est noté Γ . Supposons que nous ayons $\zeta_m \in k$, $\zeta_{m+1} \notin k$, nous fixerons un générateur topologique γ de Γ à l'aide de la formule :

$$\forall n \quad \gamma(\zeta_n) = \zeta_n^{1+\ell^m} . \quad (3)$$

Comme dans [6] nous introduirons l'anneau de séries formelles $\Lambda = \mathbb{Z}_\ell[[T]]$, étant rappelé qu'il existe un plongement de l'algèbre de groupe $\mathbb{Z}_\ell[\Gamma]$ dans Λ envoyant γ sur $1+T$. Nous utiliserons la série formelle \dot{T} définie par :

$$\dot{T} = (1+\ell^m)(1-T+T^2+\dots) - 1 . \quad (4)$$

La série \dot{T} vérifie donc :

$$(1+T)(1+\dot{T}) = 1 + \ell^m . \quad (5)$$

Désignons par M la ℓ -extension abélienne de K non ramifiée pour les places premières à ℓ maximale (cf. [6] 3.2). On sait munir $G(M/K)$ d'une structure de Λ -module de type fini. On sait aussi qu'il existe un homomorphisme de Λ -modules à noyau et conoyau finis (un tel homomorphisme est appelé un pseudo isomorphisme) :

$$G(M/K) \rightarrow \Lambda^\rho \oplus \left(\bigoplus_{i=1}^t \Lambda/(f_i)^{e_i} \right) . \quad (6)$$

Dans cette formule f_i ($i=1, \dots, t$) désigne un polynôme irréductible unitaire et distingué ou le polynôme constant ℓ , les nombres ρ et e_i ($i=1, \dots, t$) étant des entiers naturels. Les théorèmes 15 et 16 de [6] montrent que ρ est égal à r_2 . On supposera que pour chaque $i=1 \dots t$ dans la formule (6) on a $e_i > 0$.

THEOREME 1. Le défaut de la conjecture de Leopoldt δ est égal au nombre d'indices i ($i=1 \dots t$) vérifiant la condition $f_i = T$, c'est aussi le \mathbb{Z}_ℓ -rang du noyau de la multiplication par T dans le Λ -module $G(M/K)$. La conjecture de Leopoldt est équivalente à l'injectivité de cette application.

Démonstration : On sait (cf. [6] 3.2) que $G(M_O/K)$ est égal au quotient $G(M/K)/T.G(M/K)$. Le \mathbb{Z}_ℓ rang de $G(M_O/K)$ qui vaut $r_2 + \delta$ s'obtient aussi à l'aide de (6) : si $X = \Lambda$ le \mathbb{Z}_ℓ rang de X/TX vaut 1 et la multiplication par T dans X est injective ; si $X = \Lambda/(f_i)^{e_i}$ avec $f_i \neq T$ les \mathbb{Z}_ℓ -rangs de X/TX et du noyau de la multiplication par T dans X sont nuls ; si $X = \Lambda/(T)^e$ avec e entier naturel non nul, les \mathbb{Z}_ℓ -rangs de X/TX et du noyau de la multiplication par T valent 1. L'interprétation de δ donnée par le théorème 1 en résulte immédiatement. La traduction de la conjecture de Leopoldt s'en déduit à l'aide de [6] théorème 18.

Désignons par k_n la sous-extension de K/k de degré ℓ^n sur k . Le théorème 1 admet le corollaire suivant (cf. [7]) :

COROLLAIRE. Appelons δ_n le défaut de la conjecture de Leopoldt relative au corps k_n ; δ_n est une fonction croissante de n constante à partir d'un certain rang.

Démonstration : Pour appliquer le théorème 1 à k_n il faut remplacer γ par γ^n ; ainsi δ_n est le \mathbb{Z}_ℓ -rang du noyau de la multiplication par $\omega_n = (1+T)^\ell - 1$ dans le Λ -module $G(M/K)$; on doit donc considérer les polynômes f_i , cf.(6), qui divisent ω_n . Or la décomposition de ω_n en produit de facteurs irréductibles est :

$$\omega_n = T \cdot \prod_{i=1}^n \xi_i . \quad (7)$$

$$\text{Avec pour } i \geq 1, \quad \xi_i = \omega_i / \omega_{i-1} = \sum_{k=0}^{\ell-1} (1+T)^k \cdot \ell^{i-1} . \quad (8)$$

Ainsi δ_n est la somme des degrés des polynômes f_i qui sont égaux à un élément ξ_k pour un indice k inférieur ou égal à n . D'où le corollaire.

Désignons par N (respectivement par N') la ℓ -extension abélienne de K obtenue par adjonction des racines des unités de K (respectivement des unités de K pour toutes les places premières à ℓ) cf [6] 7.3. Désignons par L (respectivement par L') la ℓ -extension abélienne maximale de K qui soit non ramifiée (respectivement qui soit non ramifiée et telle que les places au-dessus de ℓ soient totalement décomposées) cf. [6] 3.4 et 4.3. Nous utiliserons ces notations dans l'énoncé et la démonstration du théorème 2.

THEOREME 2. Le défaut δ de la conjecture de Leopoldt est égal au \mathbb{Z}_ℓ -rang du noyau de la multiplication par T dans les Λ -modules $G(L/K)$ et $G(L'/K)$; il est inférieur ou égal à l'invariant λ de $G(L/K)$.

Démonstration : Ecrivons la suite exacte de groupes de Galois :

$$0 \rightarrow G(M/N') \rightarrow G(M/K) \rightarrow G(N'/K) \rightarrow 0 . \quad (9)$$

La multiplication par T étant injective dans $G(N'/K)$ ([6] théorème 15), δ est encore le \mathbb{Z}_ℓ -rang de la multiplication par T dans $G(M/N')$.

Ecrivons une décomposition analogue à (6) pour le Λ -module $G(M/N')$; il existe un homomorphisme à noyau et conoyau finis du type :

$$G(M/N') \rightarrow \bigoplus_{i=1}^p \Lambda/(g_i)^{d_i} . \quad (9)$$

Dans cette décomposition, p est un entier naturel ainsi que les nombres d_i ($i = 1 \dots p$) ; on suppose les nombres d_i strictement positifs ; les polynômes g_i vérifient les mêmes conditions que les f_i dans (6) ; la suite $g_1 \dots g_p$ est d'ailleurs une sous-suite de la suite $f_1 \dots f_t$. Le nombre δ est donc le nombre d'indice i vérifiant $g_i = T$. Pour $i = 1 \dots p$ définissons une série formelle h_i en composant g_i et \dot{T} :

$$h_i(T) = g_i(\dot{T}) . \quad (10)$$

Le résultat d'adjonction de [6] théorème 16 permet de déduire de l'homomorphisme (9) un homomorphisme jouissant des mêmes propriétés :

$$G(L'/K) \rightarrow \bigoplus_{i=1}^p \Lambda/(h_i)^{d_i} . \quad (11)$$

Ainsi δ est le nombre d'indice i vérifiant $h_i = \dot{T}$; c'est donc aussi le \mathbb{Z}_ℓ -rang du noyau de la multiplication par \dot{T} dans $G(L'/K)$. Pour $G(L/K)$ on a un résultat analogue.

On sait que pour chaque i ($i = 1 \dots p$) il existe un polynôme p_i qui vérifie les conditions citées après (6) et une unité u_i de Λ tels que h_i soit le produit de p_i par u_i . Par exemple si $h_i = \dot{T}$ on a $p_i = T - \ell^m$. L'invariant λ de $G(L'/K)$ est la somme des degrés des polynômes p_i pour $i = 1 \dots p$. Il est donc supérieur ou égal à δ ; il en est donc de même pour l'invariant λ du Λ -module $G(L/K)$.

Du théorème 2 on déduit immédiatement l'implication :

$$G(L'/K) = 0 \Rightarrow \delta = 0 . \quad (12)$$

Naturellement, la réciproque est fausse puisque les corps cyclotomiques correspondant à des nombres premiers irréguliers fournissent des exemples où δ est nul et $G(L'/K)$ infini.

Remarquons pour finir que les considérations précédentes permettent

de répondre à une question posée par K. IWASAWA à J.J. PAYAN. Cette réponse fait l'objet du théorème 3 (cf aussi [5] proposition 1).

Soient F un corps de nombres abélien et de degré fini sur le corps des rationnels \mathbb{Q} et k le corps $F(\zeta_1)$ (ou $F(\zeta_2)$ pour $\ell = 2$). Désignons par F_n le sous-corps de k_n de degré ℓ^n sur F . Appelons \mathfrak{H}_n le sous-groupe du groupe des classes des idéaux de F_n , sous-groupe engendré par les idéaux premiers au-dessus de ℓ .

THEOREME 3. Il existe un entier a tel que les groupes \mathfrak{H}_n avec $n \geq a$ soient isomorphes entre eux.

Démonstration : Il est clair qu'il suffit de s'intéresser aux ℓ -sous-groupes de Sylow \mathfrak{H}'_n des groupes \mathfrak{H}_n .

Soient F_∞ la réunion des corps F_n et Δ le groupe de Galois $G(K/F_\infty) \simeq G(k/F)$. Les corps k_n vérifiant la conjecture de Leopoldt (cf [3]), les noyaux des multiplications par les éléments ω_n de Δ dans le module $G(M/K)$ sont finis. Il en est de même pour $G(M/K)^\Delta$, sous-groupe des points fixes de $G(M/K)$ pour l'action naturelle de Δ , et donc, $G(M/K)^\Delta$ étant un Δ -module de torsion (cf [6] Lemme 25 et théorème 16), pour l'image de $G(M/K)^\Delta$ dans $G(L/K)$. Le groupe de cohomologie $H^1(\Delta, G(M/L))$ est annulé par l'ordre de Δ . Le noyau de la multiplication par ω_n (pour n quelconque) dans ce groupe est donc fini.

Il en est donc de même pour le Δ -module $G(L/K)^\Delta$ d'après la suite exacte de cohomologie :

$$G(M/K)^\Delta \rightarrow G(L/K)^\Delta \rightarrow H^1(\Delta, G(M/L)).$$

D'après [6] théorème 9, on sait que $G(L/L')^\Delta$ est annulé par ω_n pour n assez grand. On voit ainsi que ce groupe est fini. Soient L_Δ et L'_Δ les sous-extensions de L et L' abéliennes maximales sur F_∞ . Le groupe de Galois $G(L_\Delta/L'_\Delta)$ est la limite projective des groupes \mathfrak{H}'_n pour des applications surjectives déduites de la norme sur les idéaux.

D'après ce qui précède le groupe $G(L_{\Delta}/L'_{\Delta})$ est fini et est donc isomorphe aux groupes \mathfrak{H}'_n pour n assez grand.

II - ETUDE DE LA CONDITION $\dim \psi_k/k^{\times \ell} = r_2 + 1$.

Sauf indication contraire, on conserve les notations du I . On suppose en particulier que k contient ζ_1 (ou ζ_2 si $\ell = 2$). On introduit pour chaque place v de k un indice m_v tel que :

$$\zeta_{m_v} \in k_v, \quad \zeta_{m_v+1} \notin k_v .$$

Le groupe Θ_k étant trop difficile à étudier, on introduit un groupe plus gros ψ_k (cf [2]) formé des éléments α de k^{\times} tels que pour tout n le corps $k(\sqrt[n]{\alpha})$ soit inclus dans une extension cyclique de degré ℓ^n de k . On a donc :

$$\dim \psi_k/k^{\times \ell} \geq \dim \Theta_k/k^{\times \ell} = r_2 + 1 + \delta . \quad (13)$$

L'article [2] donne des exemples de corps k vérifiant la conjecture de Leopoldt. Il s'appuie sur l'implication :

$$\dim \psi_k/k^{\times \ell} = r_2 + 1 \Rightarrow \delta = 0 . \quad (14)$$

Nous allons ramener l'implication (14) à l'implication (12) en prouvant :

THEOREME 4. Soit k un corps de nombres contenant ζ_1 (et ζ_2 si $\ell = 2$). Si la dimension de $\psi_k/k^{\times \ell}$ est égale à $r_2 + 1$ alors le groupe $G(L'/K)$ est nul. La réciproque est vraie si les places au-dessus de ℓ sont non décomposées dans l'extension K/k .

Le théorème 4 résultera d'une suite de 6 lemmes. Commençons par décrire le sous-groupe ψ_k de k^{\times} .

LEMME 1. Un élément α de k^{\times} est dans ψ_k si et seulement si pour chaque place v ζ_{m_v} est norme de l'extension $k_v(\sqrt[\ell]{\alpha})/k_v$.

Démonstration : On a traduit que la condition de plongement 4 de [1] chapitre X théorème 6, le cas spécial étant exclus, devait être vérifiée pour chaque valeur de n .

LEMME 2. Si α est dans ψ_k , alors ℓ divise la valuation $v(\alpha)$ de α pour chaque place v de k première à ℓ .

Démonstration : Il suffit de se reporter à [2] démonstration de la proposition 1.2.

Le lemme suivant va nous permettre de remplacer le corps k par un corps k_n pour n assez grand.

Observons que si le nombre de plongements imaginaires de k est $2r_2$ celui de k_n est $2r_2\ell^n$. Introduisons pour chaque n , le sous-groupe ψ_n de k_n^\times défini à l'aide de k_n comme ψ_k à l'aide de k . Alors :

LEMME 3. Si la dimension de $\psi_k/k^{\times\ell}$ vaut r_2+1 , celle de $\psi_n/k_n^{\times\ell}$ (pour n entier naturel) vaut $r_2\ell^{n+1}$.

Démonstration : Nous allons la faire en 5 étapes. Pour n entier, notons μ_n le groupe des racines de 1 d'ordre une puissance de ℓ et contenues dans k_n . Désignons par G le groupe de Galois de k_n/k et choisissons un générateur σ .

■ Les groupes de cohomologie $H^1(G, \mu_n)$ et $H^2(G, \mu_n)$ sont nuls : il suffit de le voir pour $H^2(G, \mu_n)$; on prend un générateur de μ_n et on montre que sa norme est un générateur de μ_0 .

■ L'inclusion de k^\times dans k_n^\times induit une injection $k^\times/\mu_0 k^{\times\ell} \rightarrow k_n^\times/\mu_n k_n^{\times\ell}$; il s'agit de voir qu'un élément x de $k^\times \cap \mu_n k_n^{\times\ell}$ est dans $\mu_0 k^{\times\ell}$. Un tel élément peut s'écrire $x = a\ell\zeta$ avec $a \in k_n^\times$, $\zeta \in \mu_n$. Ainsi :

$$1 = x^{1-\sigma} = (a\ell\zeta)^{1-\sigma} = a^{1-\sigma} \ell^{1-\sigma} \zeta^{1-\sigma}.$$

Ceci prouve donc que $(a\ell)^{1-\sigma}$ est dans μ_n et de norme 1 : on peut

l'écrire sous la forme $\zeta'^{1-\sigma}$ avec ζ' dans μ_n . Le rapport a/ζ' est donc un élément b de k^X . Ainsi x est le produit de b^ℓ par un élément de μ_n . Comme $\mu_n \cap k^X = \mu_0$ l'injectivité annoncée est démontrée.

■ Le groupe G opère sur $k_n^X/\mu_n k_n^{X\ell}$ et les points fixes pour cette action sont dans l'image de $k^X/\mu_0 k^{X\ell}$. En effet, soit x un élément de k_n^X dont la classe est invariante. On peut trouver un élément ζ de μ_n et un élément y de k_n^X tels que $x^{1-\sigma}$ s'écrive ζy^ℓ . De là, en prenant la norme de k_n à k :

$$1 = N(x^{1-\sigma}) = N(\zeta)N(y)^\ell.$$

Ainsi $N(y)$ est dans μ_0 , c'est donc la norme d'une racine ζ' dans μ_n ; on peut trouver d'après le théorème 90 de Hilbert un élément z de k_n^X tel que :

$$y = \zeta' z^{1-\sigma}.$$

Ainsi $x^{1-\sigma}$ est le produit de $(z^\ell)^{1-\sigma}$ par une racine de l'unité dans μ_n . Cette racine, étant de norme 1, peut s'écrire sous la forme $\zeta''^{1-\sigma}$ avec un élément ζ'' de μ_n . Le quotient $x/\zeta'' z^\ell$ est donc dans k^X . La classe de x est donc dans l'image de l'application

$$k^X/\mu_0 k^{X\ell} \rightarrow k_n^X/\mu_n k_n^{X\ell}.$$

D'où le résultat annoncé.

■ Désignons par $\overline{\psi}$ et $\overline{\psi}_n$ les quotients de ψ_k et de ψ_n par leurs sous-groupes $\mu_0 k^{X\ell}$ et $\mu_n k_n^{X\ell}$. Ce qui précède montre qu'on a un homomorphisme injectif $\overline{\psi} \rightarrow \overline{\psi}_n$. Il est clair que ψ_n est un sous- G -module de k_n^X et que $\overline{\psi}_n$ est un sous G -module de $k_n^X/\mu_n k_n^{X\ell}$. Montrons que le sous-groupe des points fixes de $\overline{\psi}_n$ par l'action de G est égal à l'image de $\overline{\psi}$. Il est clair qu'il contient cette image. Soit réciproquement un élément x de k_n^X dont la classe dans $k_n^X/\mu_n k_n^{X\ell}$ est dans $\overline{\psi}_n^G$. D'après le point précédent, on peut remplacer x par un élément de k^X sans modifier sa classe. Nous allons en fait montrer que si x est dans $\psi_n \cap k^X$, alors il est dans ψ_k . Pour chaque place w de k_n introduisons l'indice m_w tel que ζ_{m_w} soit dans le complété

$k_{n,w}$ de k_n pour w , et non ζ_{m_w+1} . Le lemme 1 appliqué à $x \in \psi_n$ montre que pour chaque w le symbole de Hilbert dans $k_{n,w}, (\zeta_{m_w}, x)_w$ vaut 1. Désignons par v la place de k en dessous de w et par N_w la norme de $k_{n,w}$ à k_v . L'analogue de la 1ère étape ci-dessus appliqué à l'extension locale montre que $N_w(\zeta_{m_w})$ est une racine de k_v engendrant le même groupe que ζ_{m_v} . Considérons le symbole de Hilbert dans $k_v, (\zeta_{m_v}, x)_v$ il vaut 1 si et seulement si il en est de même pour $(N_w(\zeta_{m_w}), x)_v$, symbole encore égal à $(\zeta_{m_w}, x)_w$ qui vaut 1. Ainsi pour chaque place v de k , on a $(\zeta_{m_v}, x)_v = 1$. Donc d'après le lemme 1 x est dans ψ_k . Nous avons donc démontré l'inclusion de $\psi_n \cap k^\times$ dans ψ_k , donc aussi l'isomorphisme suivant :

$$\overline{\psi}_n^G \simeq \overline{\psi} \quad (15)$$

■ Nous pouvons maintenant démontrer le lemme 3. Si la dimension de $\psi_k/k^{\times \ell}$ est r_2+1 , celle de $\overline{\psi}$ est r_2 ; il en est donc de même pour $\overline{\psi}_n^G$ et $\overline{\psi}_n/(1-\sigma)\overline{\psi}_n$. Ceci prouve que $\overline{\psi}_n$ admet un système générateur de r_2 éléments en tant que G -module. Sa dimension comme espace vectoriel sur le corps fini à ℓ éléments est donc inférieure ou égale à $r_2 \cdot \ell^n$. Il en résulte, en utilisant aussi l'inégalité (13) pour le corps k_n , que la dimension de $\psi_n/k_n^{\times \ell}$ est $r_2 \ell^n + 1$.

Le lemme 3 permet de remplacer le corps k par un corps k_n avec n suffisamment grand. C'est ce que nous ferons pour les lemmes 4, 5, 6, ainsi que pour (19) et (31) : nous y supposerons que les places au-dessus de ℓ sont non décomposées dans l'extension K/k .

Soient S l'ensemble des places de k divisant ℓ et T un ensemble fini de places non décomposées dans k_1/k et comprenant les places de S . L'ensemble T permet de décrire ψ_k :

LEMME 4. Un élément α de k^X est dans ψ_k si et seulement si il vérifie simultanément les conditions :

1. Pour toute place v de k non dans T , ℓ divise la valuation $v(\alpha)$ de α .
2. α est norme de l'extension k_1/k .

Démonstration : Pour les places v dans T on a $\zeta_{m_v} = \zeta_m$ et les symboles de Hilbert $(\zeta_{m_v}, \alpha)_v$ et $(\alpha, \zeta_m)_v$ sont donc inverses l'un de l'autre.

Pour les places v non dans T , la condition (1) est vérifiée si α est dans ψ_k (cf Lemme 2). Cette condition implique d'ailleurs que les symboles précédents valent 1. Si α est dans ψ_k il vérifie donc les conditions (1) et (2), (cf. "théorème des normes de Hasse"). Si α vérifie les conditions (1) et (2), il vérifie les conditions du lemme 1 et est dans ψ_k .

Pour évaluer ψ_k introduisons les notations suivantes. Soit \mathfrak{R} l'ensemble des éléments de k^X vérifiant seulement la condition (1) du lemme 4. En désignant toujours par N la norme de k_1 dans k , on a :

$$\psi_k = \mathfrak{R} \cap Nk_1^X. \quad (16)$$

Désignons par \mathfrak{e} (respectivement E') l'ensemble des éléments de k^X qui sont des unités pour les places non dans T (respectivement non dans S), par \mathfrak{J} (respectivement I') le groupe des idéaux de k premiers aux places de T (respectivement de S), par \mathfrak{P} (respectivement P') l'image du sous-groupe des idéaux principaux par la surjection envoyant le groupe des idéaux dans \mathfrak{J} (respectivement dans I'). Notons \mathfrak{C} (respectivement C') le quotient $\mathfrak{J}/\mathfrak{P}$ (respectivement I'/P'). Soit \mathfrak{G} (respectivement A') son ℓ sous-groupe de Sylow. Ainsi \mathfrak{C} (respectivement C') est le quotient du groupe des classes d'idéaux de k par le sous-groupe engendré par les classes des éléments de T (respectivement de S).

Pour k_1 , on notera S_1 et T_1 les ensembles de places au-

dessus des places de S et de T ; à l'aide de S_1 , T_1 , k_1 faisons les mêmes définitions que plus haut et ajoutons un indice 1 pour distinguer les nouveaux objets : ϵ_1 , E'_1 , \mathcal{J}_1 , I'_1 etc...

Désignons par ${}_{\ell}\mathcal{C}$ le noyau de la multiplication par ℓ dans \mathcal{C} . Le sous-groupe \mathfrak{K} de k^\times intervient dans la suite exacte :

$$0 \rightarrow \epsilon/\epsilon^\ell \rightarrow \mathfrak{K}/k^{\times\ell} \rightarrow {}_{\ell}\mathcal{C} \rightarrow 0. \quad (17)$$

Expliquons seulement comment est définie la surjection ci-dessus. Si α est un élément de \mathfrak{K} , il engendre un idéal principal (α) qui se décompose à l'aide d'un idéal \mathfrak{A} premier aux places de T et d'un idéal \mathfrak{B} produit d'idéaux premiers de T :

$$(\alpha) = \mathfrak{A}^\ell \mathfrak{B}. \quad (18)$$

La surjection envoie alors la classe de α dans la classe de \mathfrak{A} dans \mathcal{C} , classe qui est dans ${}_{\ell}\mathcal{C}$.

Considérons la restriction de la surjection précédente à $\psi_k/k^{\times\ell}$, elle permet d'écrire la suite exacte :

$$0 \rightarrow \epsilon \cap Nk_1^\times / \epsilon^\ell \rightarrow \psi_k/k^{\times\ell} \rightarrow {}_{\ell}\mathcal{C}. \quad (19)$$

Remarquons alors que l'indice $[\epsilon \cap Nk_1^\times : \epsilon^\ell]$ peut s'évaluer à l'aide d'une généralisation de la formule des classes ambiges. Pour tout groupe fini X notons $[X]$ son ordre. Ici G désigne le groupe de Galois de k_1 sur k et t le nombre de places dans T .

LEMME 5. Les nombres $[\mathcal{C}]$, $[\mathcal{C}_1^G]$, t , $[\epsilon : \epsilon \cap Nk_1^\times]$ vérifient :

$$[\mathcal{C}_1^G] = \frac{\ell^{t-1} [\mathcal{C}]}{[\epsilon : \epsilon \cap Nk_1^\times]}. \quad (20)$$

Démonstration : elle se fait comme pour la formule des classes ambiges ; rappelons brièvement comment. Une simplification provient du fait que \mathcal{J}_1^G est réduit à l'image de \mathcal{J} par l'application i d'extension des idéaux (T contient S). La suite de cohomologie relative à la suite exacte reliant \mathcal{P}_1 , \mathcal{J}_1 et \mathcal{C}_1 fournit la suite exacte suivante où

on utilise la nullité de $H^1(G, \mathcal{J}_1)$:

$$\mathcal{J}_1^G \rightarrow \mathcal{C}_1^G \rightarrow H^1(G, \mathcal{P}_1) \rightarrow 0 . \quad (21)$$

D'où en tenant compte de l'égalité entre \mathcal{J}_1^G et $i(\mathcal{J})$:

$$\mathcal{C} \rightarrow \mathcal{C}_1^G \rightarrow H^1(G, \mathcal{P}_1) \rightarrow 0 . \quad (22)$$

La suite exacte reliant ϵ_1 , k_1^X et \mathcal{P}_1 fournit une suite exacte de cohomologie qui permet d'évaluer $H^1(G, \mathcal{P}_1)$ à l'aide du théorème 90 de Hilbert :

$$H^1(G, \mathcal{P}_1) \simeq \epsilon \cap Nk_1^X / N\epsilon_1 . \quad (23)$$

Elle fournit aussi la suite exacte :

$$k^X \rightarrow \mathcal{P}_1^G \rightarrow H^1(G, \epsilon_1) \rightarrow 0 .$$

D'où en faisant intervenir l'image de \mathcal{P} dans \mathcal{P}_1^G par i

$$\mathcal{P}_1^G / i(\mathcal{P}) \simeq H^1(G, \epsilon_1) . \quad (24)$$

De la double inclusion $\mathcal{J}_1^G \supset \mathcal{P}_1^G \supset i(\mathcal{P})$ et de l'égalité $\mathcal{J}_1^G = i(\mathcal{J})$ on déduit la suite exacte :

$$0 \rightarrow \mathcal{P}_1^G / i(\mathcal{P}) \rightarrow i(\mathcal{J}) / i(\mathcal{P}) \rightarrow i(\mathcal{J}) / \mathcal{P}_1^G \rightarrow 0 . \quad (25)$$

Sachant que l'application i est injective et que \mathcal{P}_1^G est égal à $\mathcal{P}_1 \cap \mathcal{J}_1^G$ donc à $\mathcal{P}_1 \cap i(\mathcal{J})$, on voit que le noyau de la surjection dans (25) est isomorphe au noyau de l'application $\mathcal{C} \rightarrow \mathcal{C}_1$ déduite de i par passage au quotient. En tenant compte de (24) on a donc obtenu la suite exacte :

$$0 \rightarrow H^1(G, \epsilon_1) \rightarrow \mathcal{C} \rightarrow \mathcal{C}_1 . \quad (26)$$

En raccordant les suites (22) et (26) et en utilisant (23) on obtient la suite exacte :

$$0 \rightarrow H^1(G, \epsilon_1) \rightarrow \mathcal{C} \rightarrow \mathcal{C}_1^G \rightarrow \epsilon \cap Nk_1^X / N\epsilon_1 \rightarrow 0 . \quad (27)$$

Cette suite exacte nous donne une relation sur les ordres des groupes :

$$[\mathcal{C}_1^G] = [\mathcal{C}] \frac{[\epsilon \cap Nk_1^X : N\epsilon_1]}{H^1(G, \epsilon_1)} = [\mathcal{C}] \frac{H^2(G, \epsilon_1)}{[\epsilon : \epsilon \cap Nk_1^X] [H^1(G, \epsilon_1)]} . \quad (28)$$

Le lemme 5 résulte alors de l'évaluation du quotient de Herbrand de ϵ_1

(cf [4] chapitre VII démonstration du théorème 8.3) : si pour chaque v dans T , d_v désigne l'ordre du groupe de décomposition dans k_1/k et n le degré de k_1/k , la formule est la suivante :

$$\frac{[H^2(G, \epsilon_1)]}{[H^1(G, \epsilon_1)]} = \frac{\prod_{v \in T} d_v}{n} . \quad (29)$$

Ce rapport vaut donc ℓ^{t-1} pour k_1/k et T d'où la formule (20).

Nous l'utiliserons sous une forme un peu modifiée :

$$[\epsilon \cap \text{Nk}_1^x : \epsilon^\ell] = \frac{[\epsilon : \epsilon^\ell]}{[\epsilon : \epsilon \cap \text{Nk}_1^x]} = \ell^{r_2+t} \cdot \frac{[c_1^G]}{[C] \ell^{t-1}} . \quad (30)$$

Soit encore :

$$[\epsilon \cap \text{Nk}_1^x : \epsilon^\ell] = \ell^{r_2+1} \frac{[c_1^G]}{[C]} . \quad (31)$$

LEMME 6. Si les places au-dessus de ℓ sont non ramifiées dans l'extension k_1/k , il existe un ensemble fini de places non décomposées T , contenant S et tel que le groupe C soit nul.

Démonstration : Il suffit d'appliquer le théorème de densité de Tchebotareff (cf [4] chapitre VIII) à l'extension composée de k_1 et du corps de classes de Hilbert de k . Ainsi dans toute classe d'idéaux de k , il existe un idéal premier de k non décomposé dans k_1/k . Dans T il suffira de mettre les places de S et celles correspondant pour chaque classe d'idéaux de k à un idéal premier du type précédent.

Démonstration du théorème 4 :

■ Supposons d'abord que $G(L'/K)$ soit nul : il en est de même pour A' et A'_1 si les places au-dessus de ℓ sont non décomposées dans K/k . A l'aide de (19) et (31) appliqués à $T = S$ on en déduit immédiatement que la dimension de $\psi_k/k^{x\ell}$ est r_2+1 .

■ Réciproquement, supposons que $\psi_k/k^{x\ell}$ soit de dimension r_2+1 . Le lemme 3 permet de supposer que l'extension K/k est totalement ramifiée pour les places de k divisant ℓ . Choisissons T de façon à ce que C soit nul (cf Lemme 6). L'hypothèse $\dim \psi_k/k^{x\ell} = r_2+1$,

(19) et (31) montre que C_1^G est nul : il en est de même pour G_1^G et G_1 . Soient $p_1 \dots p_{t-s}$ les places de T-S ($s =$ nombre d'éléments dans S) et $q_1 \dots q_{t-s}$ leurs prolongements à k_1 ; soit H_1 le sous-groupe de C_1' engendré par leurs classes ; le sous-groupe de Sylow de $C_1' = C_1'/H_1$ étant nul on aura :

$$C_1' = H_1 \cdot C_1'^{\ell} . \quad (32)$$

Observons maintenant que la norme des idéaux induit une surjection N de C_1' sur C' :

$$C' = NC_1' = (NH_1) \cdot (NC_1')^{\ell} . \quad (33)$$

Observons de plus que les idéaux p_i ($i = 1 \dots t-s$) étant inertes, la norme des idéaux q_i ($i = 1 \dots t-s$) sont les idéaux p_i^{ℓ} ($i = 1 \dots t-s$). Ceci prouve que NH_1 est en fait dans C'^{ℓ} . En conséquence, le sous-groupe de Sylow A' de C' est nul. En réutilisant (19) et (31) avec $T = S$ on déduit immédiatement la nullité de A_1^G donc de A_1' . Appliquons alors le théorème 8 de [6] : si $X = G(L'/K)$ il existe un sous- Λ -module Y de X tel qu'on ait des isomorphismes :

$$\begin{aligned} X/Y &\simeq A' \\ X/\nu_{0,1} Y &\simeq A_1' \quad \text{avec} \quad \nu_{0,1} = \sum_{i=0}^{\ell-1} (1+T)^i \end{aligned} \quad (34)$$

De $A' = A_1' = 0$ il résulte que X est égal à $\nu_{0,1} X$ donc est nul d'après le lemme de Nakayama.

Remarques :

■ Si le corps k ne possède qu'une place au-dessus de ℓ , supposée totalement ramifiée dans K/k , on sait qu'avec les notations précédentes et $T = S$, les éléments de \mathfrak{K} sont des normes de k_1/k , la suite exacte (19) s'écrit donc :

$$0 \rightarrow E'/E'^{\ell} \rightarrow \psi_k/k^{\times \ell} \rightarrow {}_{\ell}C' \rightarrow 0 . \quad (35)$$

Le rang de E'/E'^{ℓ} n'est autre que r_2+1 , donc la condition $\dim \psi_k/k^{\times \ell} = r_2+1$ entraîne que A' est trivial donc (puisqu'il n'y a qu'une place au-dessus de ℓ) que $G(L'/K)$ est aussi trivial. Le théo-

rème 4 se démontre donc facilement dans ce cas particulier.

■ Si k contient plus d'une place au-dessus de ℓ , la condition $A' = 0$ ne suffit pas à entraîner la nullité de $G(L'/K)$. Signalons le résultat rencontré dans la démonstration du théorème 4.

THEOREME 5. Supposons que les places au-dessus de ℓ soient totalement ramifiées dans l'extension K/k ; dans ces conditions, pour que $G(L'/K)$ soit nul, il faut et il suffit qu'il en soit de même pour A' et A'_1 .

On a évidemment un résultat analogue pour $G(L/K)$.

■ Supposons que ℓ soit impair et que le corps k soit quasi-réel c'est-à-dire soit extension quadratique d'un corps k^+ totalement réel. Soit k_n^+ le sous-corps réel de k_n . Notons K^+ la réunion des corps k_n^+ . Le groupe de Galois $G(K/K^+)$ est d'ordre 2, on note j son générateur. Désignons par s (respectivement s^+) le nombre de places de k_n (respectivement de k_n^+) au-dessus de ℓ , pour n assez grand.

THEOREME 6. Si $G(L'/K)$ est nul, les invariants λ et μ de $G(L/K)$ sont donnés par :

$$\mu = 0 \quad \lambda = s - s^+.$$

Démonstration : On sait que Λ possède une involution envoyant T sur \dot{T} . En composant les structures de Λ -modules de $G(L/K)$ et $G(L'/K)$ avec cette involution on obtient d'autres Λ -modules notés $G(L/K)^*$ et $G(L'/K)^*$. On sait (cf [6] théorème 14) que $G(M/N)$ (respectivement $G(M/N')$) est isomorphe à l'adjoint de $G(L/K)$ (respectivement de $G(L'/K)$). L'hypothèse $G(L'/K) = 0$ implique donc l'égalité de M et de N' . Ainsi $G(N'/N)$ est l'adjoint de $G(L/K)$.

Si X est un $G(K/K^+)$ module, notons X^+ l'ensemble des éléments x de X fixes par j et par X^- ceux vérifiant

$$jx = -x.$$

On voit alors facilement que l'adjoint de $[G(L/K)^*]^-$ est isomorphe à $G(N'/N)^+ \simeq G(N'/K)^+$. Comme groupe il est donc isomorphe à $\mathbb{Z}_\ell^{(s-s^+)}$ (cf [6] lemme 25). D'autre part, on sait d'après le théorème 3 ci-dessus appliqué à $F = k^+$ (dans le théorème 3 on avait supposé F abélien sur \mathbb{Q} de façon à ce que les corps k_n vérifient la conjecture de Leopoldt ; ici cette hypothèse est inutile d'après (12)) que $G(L/K)^+$ est fini. Ceci prouve que le groupe $G(L/K)$ est isomorphe au produit de $\mathbb{Z}_\ell^{(s-s^+)}$ par un groupe fini. Ceci prouve le théorème 6. On peut encore le préciser en utilisant [6] théorème 9 : pour n assez grand $G(L/K)$ sera annulé par $\omega_n = (1+T)\ell^n - 1$.

■ Illustrations numériques : nous reprenons les exemples de [2] qui correspondent à des corps quasi-réels.

- pour $\ell = 3$ et $k = \mathbb{Q}(\sqrt{-3}, \sqrt[m]{m})$ avec $m = -2, -5, -11, -14, -17, -35$, [2] montre que la dimension de $\psi_k/k^{\times \ell}$ est r_2+1 ; le groupe $G(L'/K)$ est donc nul et le théorème 6, étant donné que $s = 2$ et $s^+ = 1$, montre que pour le corps k on a $\mu = 0, \lambda = 1$.

- pour $\ell = 5$ et $k = \mathbb{Q}(\sqrt{-11}, \zeta_1)$, [2] montre que la dimension de $\psi_k/k^{\times \ell}$ est r_2+2 . Le groupe $G(L'/K)$ est donc non nul, bien que la nombre de classes de k soit premier à 5. Les conditions du théorème 5 ne sont donc pas vérifiées.

BIBLIOGRAPHIE

- [1] E. ARTIN et J. TATE - "Class-field theory" Benjamin 1967.
- [2] F. BERTRANDIAS et J.J. PAYAN - " Γ -extensions et invariants cyclotomiques". Annales Scient. Ec. Norm. Sup. 4e série t.5 1972 pp.517 à 543.
- [3] A. BRUMER - "On the units of algebraic number fields". Mathematika, 14 (1967) pp. 121-124.
- [4] J.W.S. CASSELS et A. FRÖHLICH - "Algebraic Number Theory". Academic Press (1967).

- [5] R. GREENBERG - "On a certain ℓ -Adic Representation". Inventiones
math. 21 (1973) pp. 117-124.
- [6] K. IWASAWA - "On \mathbb{Z}_ℓ -extensions of algebraic fields". Annals of
Math. Vol. 98 n° 2 sept. 73, pp.246-326.
- [7] L.V. KUZMIN - "The Tate Module for algebraic Number Fields". Izv.
Akad. Nauk. SSR. ser Mat. Tom.36 (1972) n° 2 et
Math. USSR Izvestija, Vol.6 (1972) n° 2.

-:-:-:-