ANNALES DE L'INSTITUT FOURIER

THONG NGUYEN-QUANG-DO

Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens

Annales de l'institut Fourier, tome 36, n° 2 (1986), p. 27-46

<http://www.numdam.org/item?id=AIF_1986__36_2_27_0>

Ann. Inst. Fourier, Grenoble
36, 2 (1986), 27-46.

SUR LA Z_p-TORSION DE CERTAINS MODULES GALOISIENS

par Thong NGUYEN-QUANG-DO

0. Introduction.

Soient k une extension finie de $\mathbf{Q}$, p un nombre premier (si $p = 2$, on suppose que k est imaginaire) et S un ensemble fini de places de k contenant les places archimédiennes et les places au-dessus de p. Au couple (k,S) on associe le pro-p-groupe abélien $X_k(S)$ (en abrégé : X_k), qui est par définition le groupe de Galois de la pro-p-extension abélienne S-ramifiée (i.e. non ramifiée en dehors de S) maximale de k. Un certain nombre de propriétés arithmétiques importantes de k se reflètent dans la structure de X_k : ainsi, la valeur du $\mathbf{Z}_p$-rang de X_k est donnée par la conjecture de Leopoldt pour k et p ([13], § 2), tandis que l'ordre de $\mathcal{T}_k$, le sous- groupe de $\mathbf{Z}_p$-torsion de X_k, est relié conjecturalement au résidu en $s = 1$ de la fonction zêta p-adique de k, quand k est réel (formule de Leopoldt-Coates, voir [3], thm. 1.3). Divers invariants numériques attachés à $\mathcal{T}_k$ (son rang, son ordre...) ont été étudiés par différents auteurs ([8], [9], [19]...). Nous nous proposons ici d'examiner la structure de $\mathcal{T}_k$ en tant que module galoisien.

Dans un premier temps, nous établissons une suite exacte reliant $\mathcal{T}_k$ d'un côté à la partie p-primaire du groupe des racines de l'unité semi-locales quotienté par le groupe des racines de l'unité globales, de l'autre au groupe de points fixes d'un certain module d'Iwasawa A'_∞ (1) (pour un énoncé précis, voir 1.1). Ce module de points fixes peut également s'interpréter comme étant la $\mathbf{Z}_p$-torsion T_k du module de Bertrandias-Payan de k, c'est-à-dire du groupe de Galois de la composée de toutes les p-extensions de k qui se plongent dans des p-extensions cycliques de degré arbitrairement grand (4.2).

Dans le cas totalement réel, la suite exacte 1.1 permet immédiatement de retrouver la formule de Leopoldt-Coates (2.2). Dans le cas d'un corps

Mots-clés : $\mathbf{Z}_p$-torsion - Leopoldt - Iwasawa - Bertrandias - Payan.

CM, elle permet d'exprimer asymptotiquement la « partie plus » des groupes de classes dans la $\mathbf{Z}_p$-extension cyclotomique (une hypothèse de Greenberg [11] affirme que cette « partie plus » se stabilise dans la tour cyclotomique) en fonction de la « partie moins » (3.4).

Pour finir, nous nous intéressons à des résultats de dualité entre les modules $\mathcal{C}_k$ et T_k et certains noyaux de la K-théorie (noyau modéré, noyau hilbertien). Ces résultats peuvent être considérés comme des compléments aux résultats de Tate [23] sur le K_2 des corps de nombres.

Notations.

S_p = ensemble des places de k divisant p et des places à l'infini.
S = un ensemble fini de places de k contenant S_p.
Σ (resp. Σ_p) = ensemble des places non archimédiennes de S (resp. S_p).
k_S = extension S-ramifiée maximale de k.
$k_S(p)$ = pro-p-extension S-ramifiée maximale de k.
$\mathcal{G}_S(k) = \mathcal{G}_S = \mathrm{Gal}(k_S/k)$ (si $p = 2$, l'hypothèse que k est totalement imaginaire permet de s'assurer de la finitude de la p-dimension cohomologique de $\mathcal{G}_S$).
$G_S(k) = G_S = \mathrm{Gal}(k_S(p)/k)$ (c'est donc le plus grand quotient de $\mathcal{G}_S$ qui soit un pro-p-groupe).
$X_k(S) = X_k = G_S^{ab}$ (l'abélianisé de G_S).
$\mathcal{C}_k(S) = \mathcal{C}_k$ = le sous-groupe de $\mathbf{Z}_p$-torsion de X_k.

Par le corps de classes, on sait que X_k est un $\mathbf{Z}_p$-module de type fini, donc $\mathcal{C}_k$ est un groupe fini.

Comme d'habitude, on notera μ_{p^n} le groupe des racines p^n-ièmes de l'unité, μ_{p^∞} la réunion des μ_{p^n} et, pour tout corps F, $\mu(F)$ le p-groupe des racines de l'unité contenues dans F. Pour tout $\mathcal{G}_S$-module M et pour tout entier i, $M(i)$ désignera le module M tordu i fois par le caractère cyclotomique. On notera $M[p^n]$ le sous-module des éléments annulés par p^n, $M\{p\}$ la partie p-primaire de M et $M^* = \mathrm{Hom}_{\mathbf{Z}_p}(M, \mathbf{Q}_p/\mathbf{Z}_p)$ le dual de Pontryagin de M.

Enfin, suivant l'usage, on notera $\mathrm{Ker}_S^i(k,M) = \mathrm{Ker}_S^i(M)$ les noyaux des homomorphismes de localisation :

$$H^i(\mathcal{G}_S, M) \to \prod_{v \in \Sigma} H^i(\mathcal{G}_v, M), \quad i = 1, 2,$$

où $\mathcal{G}_v$ est le groupe de Galois absolu du complété k_v de k en la place v.

1. $\mathscr{C}_k$ et cohomologie galoisienne.

Comme l'a fait remarquer G. Gras [8], la notion de S-ramification n'est pas une simple généralisation de la non-ramification, mais plutôt une notion « duale ». Le théorème 1.1 ci-dessous, qui est le résultat principal de cette section, précise cette « dualité ».

Introduisons d'abord quelques modules d'Iwasawa qui interviendront dans toute la suite. Soient $K = k(\mu_p)$, $K_\infty = k(\mu_\infty)$, $\Delta = \mathrm{Gal}(K/k)$, $\Gamma = \mathrm{Gal}(K_\infty/K)$, $G_\infty = \mathrm{Gal}(K_\infty/k)$ (donc $G_\infty \simeq \Gamma \times \Delta$). Soit L_∞ la pro-p-extension abélienne non ramifiée maximale de K_∞, L'_∞ la sous-extension de L_∞ où toutes les places de K_∞ au-dessus de S sont totalement décomposées. On pose

$$X_\infty = \mathrm{Gal}(L_\infty/K_\infty), \qquad X'_\infty = \mathrm{Gal}(L'_\infty/K_\infty),$$
$$A_\infty = \mathrm{Hom}(X_\infty, \mathbf{Q}_p/\mathbf{Z}_p), \qquad A'_\infty = \mathrm{Hom}(X'_\infty, \mathbf{Q}_p/\mathbf{Z}_p).$$

1.1. THÉORÈME. — *Supposons que k vérifie la conjecture de Leopoldt pour p. Nous avons alors une suite exacte*

$$1 \to \mu(k) \to \prod_{v \in \Sigma} \mu(k_v) \to \mathscr{C}_k(S) \to A'_\infty(1)^{G_\infty} \to 0$$

(Naturellement, pour tout groupe d'automorphismes G du corps k, cette suite est une suite exacte de $\mathbf{Z}_p[G]$-modules.)

Preuve. — Rappelons que, par définition, k vérifie la conjecture de Leopoldt pour p si et seulement si $\mathrm{rang}_{\mathbf{Z}_p} X_k = 1 + r_2$, où r_2 est le nombre de places complexes de k (ceci est indépendant de S, car toute $\mathbf{Z}_p$-extension est non-ramifiée en dehors de p). Cette conjecture équivaut (voir par exemple [19], § 9) à la nullité du groupe de cohomologie galoisienne $H^2(G_S, \mathbf{Q}_p/\mathbf{Z}_p)$ (ou $H^2(\mathscr{G}_S, \mathbf{Q}_p/\mathbf{Z}_p)$, c'est la même chose). La suite exacte de G_S-modules (avec action triviale)

$$0 \to \mathbf{Z}/p^m\mathbf{Z} \to \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{p^m} \mathbf{Q}_p/\mathbf{Z}_p \to 0$$

donne par cohomologie la suite exacte

$$\cdots \to H^1(G_S, \mathbf{Q}_p/\mathbf{Z}_p) \xrightarrow{p^m} H^1(G_S, \mathbf{Q}_p/\mathbf{Z}_p) \to H^2(G_S, \mathbf{Z}/p^m\mathbf{Z}) \to 0.$$

Par dualité on obtient des isomorphismes

$$H^2(G_S, \mathbf{Z}/p^m\mathbf{Z})^* \simeq \mathrm{Ker}(X_k \xrightarrow{p^m} X_k),$$

donc pour m assez grand, un isomorphisme

$$\mathcal{C}_k \simeq H^2(G_S, \mathbf{Z}/p^m\mathbf{Z})^* \simeq \varinjlim_m H^2(G_S, \mathbf{Z}/p^m\mathbf{Z})^*.$$

Le problème revient donc à décrire le module $H^2(\mathcal{G}_S, \mathbf{Z}/p^m\mathbf{Z})^*$ (ou $H^2(\mathcal{G}_S, \mathbf{Z}/p^m\mathbf{Z})^*$, c'est la même chose). Or la suite exacte longue de localisation de Poitou-Tate ([12], 1.3) s'écrit

$$0 \to H^0(\mathcal{G}_S, \mu_{p^m}) \to \prod_{v\in\Sigma} H^0(\mathcal{G}_v, \mu_{p^m}) \prod_{v\in S-\Sigma} \hat{H}^0(\mathcal{G}_v, \mu_{p^m})$$
$$\to H^2(\mathcal{G}_S, \mathbf{Z}/p^m\mathbf{Z})^* \to H^1(\mathcal{G}_S, \mu_{p^m}) \to \prod_{v\in\Sigma} H^1(\mathcal{G}_v, \mu_{p^m}) \to \cdots$$

c'est-à-dire :

$$1 \to \mu(k) \to \prod_{v\in\Sigma} \mu(k_v) \to \mathcal{C}_k \to \mathrm{Ker}^1_S(\mu_{p^m}) \to 0 \quad \text{pour} \quad m \quad \text{assez grand.}$$

Comme $\mathcal{C}_k$ est fini, cette suite exacte montre que les groupes $\mathrm{Ker}^1_S(\mu_{p^m})$ (qui sont finis) se stabilisent à partir d'un certain rang. En posant $\mathrm{Ker}^1_S(\mu_{p^\infty}) = \varinjlim_m \mathrm{Ker}^1_S(\mu_{p^m})$ on obtient alors la suite exacte :

$$1 \to \mu(k) \to \prod_{v\in\Sigma} \mu(k_v) \to \mathcal{C}_k \to \mathrm{Ker}^1_S(\mu_{p^\infty}) \to 0.$$

Reste à identifier le module $\mathrm{Ker}^1_S(\mu_{p^\infty})$. On sait que

$$H^1(G_\infty, \mu_{p^\infty}) = H^2(G_\infty, \mu_{p^\infty}) = 0,$$

car pour une extension cyclotomique L/K, i.e. une extension galoisienne L/K telle que $L = K(\mu(L))$, le $\mathrm{Gal}(L/K)$-module $\mu(L)$ est cohomologiquement trivial ([12], 7-1). Comme K_∞ contient μ_{p^∞}, on obtient par inflation-restriction un isomorphisme

$$H^1(\mathcal{G}_S, \mu_{p^\infty}) \simeq H^1(k_S/K_\infty, \mu_{p^\infty})^{G_\infty}.$$

Mais $H^1(k_S/K_\infty, \mu_{p^\infty}) = \mathrm{Hom}(\mathrm{Gal}(k_S/K_\infty), \mathbf{Q}_p/\mathbf{Z}_p)(1)$. La théorie de Kummer permet alors de conclure. Q.E.D.

1.2. *Remarques.* — i) Au cours de la preuve, on a montré en fait l'équivalence suivante : k vérifie la conjecture de Leopoldt si et seulement si les groupes $\mathrm{Ker}^1_S(\mu_{p^m})$ se stabilisent (voir [17], coroll. 2, où la démonstration est beaucoup plus compliquée).

ii) Si k contient μ_{p^m}, on voit facilement que $\mathrm{Ker}^1_S(\mu_{p^m}) \simeq \mathrm{Hom}(C\ell_S(k), \mu_{p^m})$, où $C\ell_S(k)$ est le quotient du groupe des

classes d'idéaux de k par le sous-groupe engendré par les classes des idéaux correspondant aux places de Σ. Au cours de la preuve, on a donc montré, sous l'hypothèse $\mu_{p^m} \subset k$, l'existence d'une suite exacte :

$$1 \to \mu_{p^m} \to \prod_{v \in \Sigma} \mu_{p^m} \to \mathcal{T}_k[p^m] \to \mathrm{Hom}\,(C\ell_S(k), \mu_{p^m}) \to 0.$$

Cette suite exacte est bien connue en K-théorie, du moins pour l'exposant p ([15], § 2). Si k ne vérifie pas la conjecture de Leopoldt, la suite reste valable en remplaçant $\mathcal{T}_k[p^m]$ par $H^2(\mathcal{G}_S, \mathbf{Z}/p^m\mathbf{Z})^*$.

Le théorème 1.1 permet facilement de retrouver un certain nombre de résultats connus sur $\mathcal{T}_k$ (voir [8], § 4 ou [19], § 9). Nous nous contenterons de signaler le corollaire suivant, qui précise et étend les théorèmes de Miki [17] et Gillard [7] :

1.3. COROLLAIRE (Gillard [7], Miki [17]). — *Supposons que k contient μ_p (donc que $k = K$). Les conditions suivantes sont équivalentes :*

i) $\mathcal{T}_k(S) \simeq (\prod_{v \in \Sigma} \mu(k_v))/\mu(k)$

ii) $A'_\infty = (0)$, *c'est-à-dire* $L'_\infty = K_\infty$

iii) $C\ell_S(K_n) = (0)$ *pour tous les étages* K_n *de la tour cyclotomique* K_∞/K *à partir d'un certain rang.*

Preuve. — $A'_\infty = (0) \Leftrightarrow A'_\infty(1) = (0) \Leftrightarrow A'_\infty(1)^\Gamma = (0)$ (car A'_∞ est le dual d'un pro-p-groupe et Γ est un pro-p-groupe). Le reste de la démonstration est immédiat. Q.E.D.

Dans [17], H. Miki donne un certain nombre d'exemples de corps k (notamment des corps diédraux) vérifiant les conditions de 1-3 pour $p = 3,5$. Nous donnerons plus loin (2.3) des exemples systématiques dans le cas $p = 2$.

Nous terminons cette section par une propriété « galoisienne ».

1.4. PROPOSITION. — *Soit L/k une extension galoisienne finie contenue dans $k_S(p)$, de groupe de Galois G. Supposons que L (donc aussi k) vérifie la conjecture de Leopoldt. Alors l'homomorphisme de transfert $X_k \to X_L$ induit un isomorphisme $\mathcal{T}_k(S) \xrightarrow{\sim} \mathcal{T}_L(S)^G$.*

Preuve. — On sait que $cd\, G_S(k) \leqslant 2$. Soit D le module dualisant de $G_S(k)$; c'est aussi celui de $G_S(L)$, puisque $G_S(L)$ est d'indice fini dans $G_S(k)$ ([21], I-29). Par définition du module dualisant, on a des

isomorphismes fonctoriels

$$H^2(G_S(k),\mathbf{Z}/p^n\mathbf{Z})^* \simeq \mathrm{Hom}\,(\mathbf{Z}/p^n\mathbf{Z},D)^{G_S(k)}$$

et

$$H^2(G_S(L),\mathbf{Z}/p^n\mathbf{Z})^* \simeq \mathrm{Hom}\,(\mathbf{Z}/p^n\mathbf{Z},D)^{G_S(L)}.$$

La proposition en résulte moyennant l'hypothèse de Leopoldt. Q.E.D.

Notons que l'hypothèse de S-ramification imposée à l'extension L/k *n'est pas une hypothèse restrictive.* Si elle n'est pas vérifiée, il n'y a qu'à considérer l'ensemble T formé des places de S et des places qui se ramifient dans L/k. La relation entre $\mathcal{C}_k(S)$ et $\mathcal{C}_k(T)$ sera donnée en 4.3. A partir de là, on pourrait retrouver sans trop de difficultés un certain nombre de résultats de G. Gras reliant les groupes $\mathcal{C}_k$ et $\mathcal{C}_L^G$ ([9], § 5). Nous n'entrons pas dans les détails.

2. $\mathcal{C}_k$ et formules analytiques.

Pour l'essentiel, les « formules analytiques » dont il est question relient, d'une part les ordres de $\mathcal{C}_k$ et de certains groupes associés, d'autre part les valeurs en 0 des séries caractéristiques de certains modules d'Iwasawa. *On supposera dans toute cette section que* $S = S_p$ (voir cependant 4.3).

Fixons d'abord quelques notations. Rappelons que $K = k(\mu_p)$, $\Delta = \mathrm{Gal}\,(K/k)$, $\Gamma = \mathrm{Gal}\,(K_\infty/K)$, $G_\infty = \mathrm{Gal}\,(K_\infty/k) \simeq \Gamma \times \Delta$. On désigne par e_i les idempotents orthogonaux habituels de l'algèbre $\mathbf{Z}_p[\Delta]$. On identifie l'algèbre complète $\mathbf{Z}_p[\![\Gamma]\!]$ à l'algèbre des séries formelles $\Lambda = \mathbf{Z}_p[\![T]\!]$ par le choix d'un générateur topologique γ de Γ. Comme dans la section précédente, A_∞ est le dual de Pontryagin du groupe de Galois X_∞ de la pro-p-extension abélienne non ramifiée maximale de K_∞. Pour tout i, on note $g_i(T)$ la série caractéristique du Λ-module

$$\mathrm{Hom}\,(e_iA_\infty,\mathbf{Q}_p/\mathbf{Z}_p) \qquad \text{et} \qquad G_i(T) = g_i((1+T)^{-1}-1).$$

Soit $u = \chi(\gamma)$, où χ est le caractère décrivant l'action de Γ sur μ_{p^∞} (rappelons que $u \in 1 + p\mathbf{Z}_p$). Nous appellerons $Z_p(s)$ la fonction p-adique définie par :

$$s \in \mathbf{Z}_p - \{1\} \to Z_p(s) = G_1(u^s-1)/(u^s-u)$$

(la « conjecture principale » de la théorie d'Iwasawa affirme que $Z_p(s)$ est essentiellement la fonction zêta p-adique associée à k; voir [3]).

2.1. PROPOSITION. — *Supposons que k est un corps totalement réel (donc $p \neq 2$ avec nos conventions) vérifiant la conjecture de Leopoldt. Alors* $G_1(u-1) \sim |\mathcal{T}_k| \sim \rho_p|\mu(K)|$ *où* $\rho_p = \dfrac{hR}{\sqrt{d}} \prod_{v|p} (1-(Nv)^{-1})$, *$h$ est le nombre de classes, R le régulateur p-adique, d la valeur absolue du discriminant de k, et le signe $\sim$ signifie l'égalité à une unité p-adique près.*

Preuve. — Il suffit d'appliquer 1.1 et de calculer l'ordre de $A'_\infty(1)^{G_\infty}$. On a :

$$(A'_\infty(1))^{G_\infty} = (X'_\infty{}^*(1)^\Delta)^\Gamma = ((e_1X'_\infty)(-1)^*)^\Gamma = (e_1X'_\infty(-1)_\Gamma)^* .$$

Comme k est réel, $K = k(\mu_p)$ est un corps CM et l'on sait que $(e_iX'_\infty)(-i)$ n'a pas de sous-module fini non nul pour i impair. De plus, $e_1X'_\infty(-1)^\Gamma$ est fini par l'hypothèse de Leopoldt. Un lemme classique ([3], App.) montre alors que $e_1X'_\infty(-1)^\Gamma = (0)$ et que $|e_1X'_\infty(-1)_\Gamma| \sim f_1(u^{-1}-1)$, où $f_1(T)$ est la série caractéristique de $e_1X'_\infty$. Or la relation entre $f_1(T)$ et $g_1(T)$ est connue (voir [13], thm. 9 ou [25], pp. 8-19). Tous calculs faits, on trouve que $g_1(u^{-1}-1) \sim f_1(u^{-1}-1).\prod_{v|p} |\mu(k_v)|$. La suite exacte 1.1 permet de conclure que $G_1(u-1) \sim |\mathcal{T}_k|$ car $|\mu(k)| = 1$ sous nos hypothèses. Quant à l'équivalence $|\mathcal{T}_k| \sim \rho_p.|\mu(K)|$, elle provient d'un calcul classique de Coates ([3], App.).

2.2 *Rappels sur le calcul de $|\mathcal{T}_k|$.* — Revenons au cas général (k non forcément réel et p non forcément impair). Soient $\mathcal{U} = \mathcal{U}_k$ le produit des groupes des unités principales des k_v, pour toutes les places $v|p$; $E = E_k$ le groupe des unités de k dont l'image par l'application diagonale est dans $\mathcal{U}$. On identifie E à un sous-groupe de $\mathcal{U}$, et l'on note $\bar{E}$ son adhérence. Introduisons les corps suivants :

$\hat{k}$ = p-extension abélienne non ramifiée maximale de k,
$\tilde{k}$ = composé de toutes les $\mathbf{Z}_p$-extensions de k,
$\check{k}$ = sous-extension abélienne maximale de $k_S(p)$.

Par définition, $\mathcal{T}_k = \mathrm{Gal}(\check{k}/\tilde{k})$ et par le corps de classes, $\mathrm{Gal}(\check{k}/\hat{k}) \simeq \mathcal{U}/\bar{E}$. Nous en déduisons immédiatement que $\mathrm{Gal}(\check{k}/\hat{k}\tilde{k}) \simeq t(\mathcal{U}/\bar{E})$, où $t(.)$ désigne la $\mathbf{Z}_p$-torsion. Posons $h_k = h = |\mathrm{Gal}(\hat{k}/k)|$ (le p-nombre de classes) et $\tilde{h}_k = \tilde{h} = |\mathrm{Gal}(\hat{k} \cap \tilde{k}/k)|$. Nous obtenons ainsi la formule

$$|\mathcal{T}_k| = \frac{h}{\tilde{h}} |t(\mathcal{U}/\bar{E})| .$$

2.3. PROPOSITION. — *Soient* $p = 2$ *et* k *un corps quadratique imaginaire. Alors* k *vérifie les conditions équivalentes du corollaire* 1.5 *si et seulement si* k *est l'un des corps suivants :*

i) $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$

ii) $\mathbf{Q}(\sqrt{-q})$, q *premier,* $q \equiv 3, 5, 7 \pmod 8$

iii) $\mathbf{Q}(\sqrt{-2q})$, q *premier,* $q \equiv 3, 5 \pmod 8$

iv) $\mathbf{Q}(\sqrt{-qr})$, q, r *premiers,* $q \equiv -r \equiv 3 \pmod 8$.

(Notons que dans tous les cas, $|\mathcal{C}_k| = 1$ ou 2.)

Preuve. — Pour un corps quadratique imaginaire, il est clair que $t(\mathcal{U}/\tilde{\mathrm{E}}) \simeq t(\mathcal{U})/t(\tilde{\mathrm{E}}) = \prod_{v|p} (\mu(k_v))/\mu(k)$. Alors le corps k vérifie la condition i) du corollaire 1.5 si et seulement si $h = \tilde{h}$, i.e. $\hat{k} \subset k$. Or cette dernière condition a été étudiée par G. Gras, qui a déterminé tous les corps quadratiques imaginaires pour lesquels elle est vérifiée ([10], théor. 2.3). Q.E.D.

En complément du corollaire 2.2, donnons maintenant une « formule analytique p-adique » pour h^-. Supposons que $p \neq 2$ et que k est un corps CM. Pour tout $\mathcal{G}_S$-module M, on désigne comme d'habitude par M^+ (resp. M^-) le sous-module formé des éléments laissés fixes (resp. renversés) par la conjugaison complexe.

On définit les séries $\mathrm{G}'_i(\mathrm{T})$ relatives au module X'_∞ de la même manière que les séries $\mathrm{G}_i(\mathrm{T})$ relatives au module X_∞.

2.4. PROPOSITION. — *Supposons que* $p \neq 2$ *et que* k *est un corps* CM *vérifiant la conjecture de Leopoldt et contenant* μ_p. *Soient*

$$h^- = |\mathrm{Gal}(\hat{k}/k)^-| \qquad \text{et} \qquad \tilde{h}^- = |\mathrm{Gal}(\hat{k} \cap \tilde{k}/k)^-|.$$

Posons $\mathrm{G}'_+(\mathrm{T}) = \prod_{i \text{ pair}} \mathrm{G}'_i(\mathrm{T})$. *Alors* $h^- \sim \tilde{h}^- . \mathrm{G}'_+(u-1) . |\mathrm{X}'^+_\infty(-1)^\Gamma|$.

Preuve. — D'après 1.1, on a une suite exacte

$$1 \to \mu(k)^- \to \prod_{v|p} \mu(k_v)^- \to \mathcal{C}_k^- \to (\mathrm{A}'_\infty(1)^\Gamma)^- \simeq (\mathrm{A}'^+_\infty(1))^\Gamma \to 0.$$

Or $(\mathrm{A}'^+_\infty(1))^\Gamma$ est dual de $\mathrm{X}'^+_\infty(-1)_\Gamma$. Comme dans 2.1, on a $\mathrm{G}'_+(u-1) \sim |\mathrm{X}'^+_\infty(-1)_\Gamma| / |\mathrm{X}'_\infty{}^+(-1)^\Gamma|$. On termine la démonstration en

remarquant que, d'après 2.2, $|\mathscr{C}_k^-| = \frac{h^-}{\tilde{h}^-} |t(\mathscr{U}/\tilde{\mathrm{E}})^-|$ et que $t(\mathscr{U}/\tilde{\mathrm{E}})^- \simeq (\prod_{v|p} \mu(k_v)^-)/\mu(k)^-$ pour un corps CM. Q.E.D.

2.5. *Remarques.* — i) La quantité $\tilde{h}^-$ possède une expression en termes des « logarithmes p-adiques » introduits par G. Gras ([8], théor. 4.2).

ii) La démonstration de 2.4 donne un critère de nullité de X'^+_∞. On a : $X'^+_\infty = (0)$ si et seulement si $h^- = \tilde{h}^-$, si et seulement si $\mathrm{Gal}(\tilde{k}\tilde{k}/\tilde{k})^- = (0)$.

iii) L'hypothèse de Greenberg [11] affirme que X'^+_∞ est fini. En admettant cette hypothèse, la formule de la proposition se réduit à $h^- \sim \tilde{h}^- . |X'^+_\infty(-1)^\Gamma|$. En montant les étages de la tour cyclotomique, on constate que les quotients $h_n^- / \tilde{h}_n^-$ se stabilisent (voir aussi 3.4).

3. $\mathscr{C}_k$ et modules d'Iwasawa.

Les assertions de 2.5 iii) peuvent s'exprimer plus commodément en termes d'invariants d'Iwasawa. Revenons au cas général et introduisons un troisième module d'Iwasawa en posant $Y_\infty = \mathrm{Gal}(M_\infty / K_\infty)$, où M_∞ est la pro-p-extension abélienne S-ramifiée maximale de K_∞.

Soient Σ_∞ l'ensemble des places de K_∞ au-dessus de Σ. Pour toute place $v \in \Sigma_\infty$, soient Γ_v le sous-groupe de décomposition de Γ relatif à v et $\Lambda_v = \mathbf{Z}_p[\![\Gamma_v]\!]$. Pour tout Λ_v-module M, on pose $\mathrm{Ind}_v M = M \underset{\Lambda_v}{\otimes} \Lambda$.

3.1. PROPOSITION. — *Supposons que toutes les extensions intermédiaires de la $\mathbf{Z}_p$-extension cyclotomique de K vérifient la conjecture de Leopoldt. Nous avons alors une suite quasi-exacte de Λ-modules*

$$0 \to T(\mu_{p^\infty}) \to \prod_{v \in \Sigma_\infty} \mathrm{Ind}_v T(\mu_{p^\infty}) \to t_\Lambda(Y_\infty) \to \overset{\circ}{\overbrace{(X'_\infty(-1))}} \to 0$$

où $T(.)$ est le module de Tate, $t_\Lambda(.)$ la Λ-torsion, et $\mathring{X}$ désigne le module X avec la nouvelle action $\gamma \circ x = \gamma^{-1} x$.

(On trouve dans [13] et [25] des suites exactes analogues, mais qui vont *en sens inverse.*)

Preuve. – Soit γ un générateur topologique de Γ. Pour tout entier $n \geqslant 1$, soit K_n le corps fixe de γ^{p^n}. Posons $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$, $G_n = \mathrm{Gal}(K_n/K)$, $\omega_n = \gamma^{p^n} - 1$. Passons à la limite projective sur les suites exactes (1.1) associées à la tour d'extensions K_n/K.

i) On sait que Y_∞ est un Λ-module de rang égal à r_2 (= le nombre de places complexes de K) et ne possède pas de sous-module fini non nul (voir [13], § 8). On a donc, d'après le théorème de structure, une suite exacte :

$$0 \to Y_\infty \to \Lambda^{r_2} \oplus t_\Lambda(Y_\infty) \to F \to 0, \qquad \text{où} \qquad F \text{ est fini.}$$

La conjecture de Leopoldt pour K_n peut s'exprimer en disant que ω_n est disjoint du diviseur de Y_∞ ([13], § 11). En appliquant le lemme du serpent, on obtient alors, pour tout $n \geqslant 1$, des quasi-isomorphismes

$$(Y_\infty)_{\Gamma_n} \approx \mathbf{Z}_p[G_n]^{r_2} \oplus (t_\Lambda(Y_\infty))_{\Gamma_n},$$

avec noyaux et conoyaux *bornés*. Un simple calcul de $\mathbf{Z}_p$-rangs (en se rappelant que les K_n vérifient la conjecture de Leopoldt) montre que

$$t_{\mathbf{Z}_p}((Y_\infty)_{\Gamma_n}) \approx (t_\Lambda(Y_\infty))_{\Gamma_n}, \qquad \text{avec noyaux et conoyaux bornés.}$$

Or $\Gamma_n \simeq X_{K_n}/(Y_\infty)_{\Gamma_n}$, donc $t_{\mathbf{Z}_p}((Y_\infty)_{\Gamma_n}) = t_{\mathbf{Z}_p}(X_{K_n}) = \mathcal{C}_{K_n}$.

En repassant à la limite projective sur les K_n, on obtient un quasi-isomorphisme de Λ-modules :

$$\varprojlim_n \mathcal{C}_{K_n} \approx t_\Lambda(Y_\infty).$$

ii) Pour tout $n \geqslant 1$, on a : $A'_\infty(1)^{\Gamma_n} = \mathrm{Hom}(X'_\infty(-1)_{\Gamma_n}, \mathbf{Q}_p/\mathbf{Z}_p)$.

Une autre forme de la conjecture de Leopoldt pour K_n est que ω_n est disjoint du diviseur de $X'_\infty(-1)$. En utilisant les propriétés de l'adjoint ([13], § 1), on aura $\varinjlim_n A'_\infty(1)^{\Gamma_n} \simeq \alpha(X'_\infty(-1))$, où $\alpha(.)$ désigne l'adjoint. Mais l'on sait que $\alpha(X) \approx \overset{\circ}{X}$ pour tout Λ-module X, donc

$$\varinjlim_n A'_\infty(1)^{\Gamma_n} \approx \overset{\circ}{X'_\infty(-1)}.$$

Le reste de la démonstration est évident. Q.E.D.

Soient λ, μ les invariants d'Iwasawa associés à Y_∞, et soient λ, μ (resp. λ', μ') ceux attachés à X_∞ (resp. X'_∞). Posons $s_\infty = |\Sigma_\infty|$. Si K est un corps CM et $p \neq 2$, soient s_∞^+ la quantité analogue pour K_∞^+ et $s_\infty^- = s_\infty - s_\infty^+$.

3.2. COROLLAIRE. — *On a les relations :* $\bar{\mu} = \mu$, $\bar{\lambda} = \lambda' + s_\infty - 1$.

Si $p \neq 2$ *et* K *est un corps* CM, *on a :*

$\bar{\mu}^+ = \mu'^-$, $\bar{\mu}^- = \mu'^+$, $\bar{\lambda}^- = \lambda'^+ + s_\infty^+ - 1$, $\bar{\lambda}^+ = \lambda'^- + s_\infty^-$.

Preuve. — C'est immédiat à partir de 3.1.

3.3. *Remarque.* — Les relations entre les invariants de X_∞ et X'_∞ sont connues ([13], [25]). On a :

$$\mu = \mu' \quad \text{et} \quad 0 \leqslant \lambda - \lambda' \leqslant s_\infty - 1.$$

Si $p \neq 2$ et K est un corps CM, on a :

$$\mu^+ = \mu'^+, \quad \mu^- = \mu'^-, \quad \lambda^- = \lambda'^- + s_\infty^-, \quad \lambda^+ = \lambda'^+.$$

En combinant avec 3.2, on en tire en particulier que $\bar{\lambda}^+ = \lambda^-$ et $\bar{\lambda}^- = \lambda^+ + s_\infty^+ - 1$.

Revenons maintenant aux notations $\tilde{k}$, $\hat{k}$, etc... de la dernière partie du § 2. Posons $\tilde{X}_\infty = \varprojlim_n \mathrm{Gal}(\hat{K}_n \cap \tilde{K}_n / K_n)$, et soient $\tilde{\lambda}, \tilde{\mu}$ les invariants associés.

3.4. PROPOSITION. — *Supposons que* $p \neq 2$, *que* K *est un corps* CM *et que la conjecture de Leopoldt est vérifiée à tous les étages de la tour cyclotomique* K_∞ / K. *Nous avons alors une suite quasi-exacte de* Λ-*modules :*

$$0 \to \overset{\circ}{\widehat{X'^+_\infty(-1)}} \to X_\infty^- \to \tilde{X}_\infty^- \to 0.$$

En particulier, $\lambda^- = \tilde{\lambda}^- + \lambda^+$, $\mu^- = \tilde{\mu}^- + \mu^+$.

Preuve. — On a vu en 2.4 que $\mathrm{Gal}(\hat{K}_n / \hat{K}_n \cap \tilde{K}_n)^- \simeq (A'^+_\infty(1))^{\Gamma_n}$. En passant à la limite dans la tour cyclotomique, on obtient alors une suite exacte de Λ-modules :

$$0 \to \varprojlim_n (A'^+_\infty(1))^{\Gamma_n} \to X_\infty^- \to \tilde{X}_\infty^- \to 0.$$

Comme dans 3.1, $\varprojlim_n (A'^+_\infty(1))^{\Gamma_n} \approx \overset{\circ}{\widehat{X'^+_\infty(-1)}}$. Q.E.D.

3.5. *Remarque.* — L'hypothèse de Greenberg équivaut à $\lambda^+ = \mu^+ = 0$. En fait, comme X_∞^- n'a pas de sous-module fini non nul, il résulte facilement de 3.4 qu'elle équivaut à l'isomorphisme $X_\infty^- \simeq \tilde{X}_\infty^-$.

4. T_k et problèmes de plongement.

Revenons aux hypothèses et notations du § 1. Nous allons interpréter $A'_\infty(1)^{G_\infty}$ comme étant le module de $\mathbf{Z}_p$-torsion T_k d'un certain module galoisien introduit primitivement par Bertrandias-Payan [2]. Dans [14], J.-F. Jaulent le montre par des méthodes de K-théorie algébrique. Nous le montrons ici par des considérations cohomologiques.

Une p-extension L/K (forcément cyclique) sera dite *infiniment plongeable* si pour tout entier n, elle se plonge dans une extension cyclique de k de degré p^n. Elle sera dite *$\mathbf{Z}_p$-plongeable* si elle se plonge dans une $\mathbf{Z}_p$-extension de k. Notons que, pour des extensions de corps locaux, ces deux notions coïncident, parce que le groupe de Galois de la p-extension maximale d'un corps local est topologiquement de type fini. Rappelons le résultat suivant ([2], [7]), analogue au « principe de Hasse » :

4.1. LEMME. — *Une extension L/k est infiniment plongeable si et seulement si les extensions locales L_v/k_v sont $\mathbf{Z}_p$-plongeables, pour toute place finie v.*

Définissons maintenant BP_k, *le module de Bertrandias-Payan de k*, comme étant le groupe de Galois du composé de toutes les p-extensions infiniment plongeables de k.

4.2. THÉORÈME. — *Avec les hypothèses et les notations de* 1.1, *on a une suite exacte :*

$$1 \to \mu(k) \to \prod_{v \in \Sigma} \mu(k_v) \to \mathcal{C}_k(S) \to T_K \to 0,$$

où T_k est la $\mathbf{Z}_p$-torsion du module de Bertrandias-Payan BP_k. Autrement dit, le module $A'_\infty(1)^{G_\infty}$ est isomorphe à T_k. En particulier, il ne dépend pas de S (*pourvu que* $S \supset S_p$).

Preuve. — i) Montrons d'abord que BP_k est un quotient de $X_k = X_k(S)$: une extension locale L_v/k_v, pour $v \nmid p$, est $\mathbf{Z}_p$-plongeable si et seulement si elle est non ramifiée (puisque, pour $v \nmid p$, la seule $\mathbf{Z}_p$-extension de k_v est la $\mathbf{Z}_p$-extension non ramifiée maximale). Le lemme 4.1 peut donc se réénoncer comme suit : L/k est infiniment plongeable $\Leftrightarrow$ L_v/k_v est $\mathbf{Z}_p$-plongeable pour toute $v \mid p$, non ramifiée pour toute $v \nmid p$. Donc BP_k est bien un quotient de X_k. En fait, on a montré plus : notons $(.)^*$ le dual de Pontryagin, X_v le groupe de Galois de la pro-p-

extension abélienne maximale de k_v (c'est l'analogue local de X_k) et, pour tout caractère $\chi \in X_k^*$, notons χ_v le caractère de X_v^* obtenu par restriction. Le lemme 4.1 modifié permet de décrire le dual de BP_k dans X_k^* en fonction des sous-groupes divisibles maximaux $(X_v^*)_{\mathrm{div}}$:

$$BP_k^* = \{\chi \in X_k^* / \chi_v \in (X_v^*)_{\mathrm{div}}, \forall v \in \Sigma\}.$$

ii) Considérons l'homomorphisme $\varphi : X_k^* \to \prod_{v \in \Sigma} X_v^*/(X_v^*)_{\mathrm{div}}$ déduit de la restriction. D'après i), $\mathrm{Ker}\,\varphi = BP_k^*$. Or φ passe au quotient et induit un homomorphisme $\bar{\varphi} : X_k^*/(X_k^*)_{\mathrm{div}} \to \prod_{v \in \Sigma} X_v^*/(X_v^*)_{\mathrm{div}}$. Il est clair que $\mathrm{Ker}\,\bar{\varphi} = BP_k^*/(X_k^*)_{\mathrm{div}} \simeq T_k^*$. Mais l'homomorphisme dual $\bar{\varphi}^*$ n'est autre que l'homomorphisme $\prod_{v \in \Sigma} \mu(k_v) \to \mathcal{C}_k$ du théorème 1.1. Q.E.D.

4.3. COROLLAIRE. — *On a une suite exacte, pour tout* $S \supset S_p$:

$$1 \to \prod_{v \in S - S_p} \mu(k_v) \to \mathcal{C}_k(S) \to \mathcal{C}_k(S_p) \to 1.$$

Preuve. — On écrit la suite exacte de 4.2 pour S et S_p et l'on applique le lemme du serpent. Q.E.D.

4.4. *Remarques.* — Le résultat du corollaire pourrait aussi se déduire du théorème d'O. Neumann [18], qui est l'analogue pour les corps de nombres du « théorème d'existence » de Riemann (voir 5.1). On aurait pu aussi montrer directement 4.3 en calculant les ordres de $\mathcal{C}_k(S)$ et $\mathcal{C}_k(S_p)$ (« formules analytiques » de [3]).

ii) Si k ne vérifie pas la conjecture de Leopoldt, 4.3 reste valable en remplaçant $\mathcal{C}_k(S)$ par $H^2(\mathcal{G}_S, \mathbf{Z}_p)^* = (\varprojlim H^2(\mathcal{G}_S, \mathbf{Z}/p^m\mathbf{Z}))^*$ et $\mathcal{C}_k(S_p)$ par $H^2(\mathcal{G}_{S_p}, \mathbf{Z}_p)^*$.

Soit $Y_\infty(S)$ (resp. $Y_\infty(S_p)$) le groupe de Galois de la pro-p-extension abélienne S-ramifiée (resp. p-ramifiée) maximale de K. On note $\lambda(S)$, $\mu(S)$, $\lambda(S_p)$, $\mu(S_p)$ les invariants d'Iwasawa attachés à ces modules.

4.5. COROLLAIRE (comparer à [25], 5.6). — *Supposons que la conjecture de Leopoldt est vérifiée pour toutes les extensions intermédiaires de la tour cyclotomique* K_∞/K. *Nous avons une suite quasi-exacte de* Λ*-modules :*

$$0 \to \prod_v{}' \mathrm{Ind}_v\, T(\mu_{p^\infty}) \to t_\Lambda Y_\infty(S) \to t_\Lambda Y_\infty(S_p) \to 0,$$

où le produit $\prod_v'$ *est étendu à toutes les places de* K_∞ *au-dessus des places* v *de* $S - S_p$. *En particulier,*

$$\bar{\mu}(S) = \bar{\mu}(S_p) \qquad \text{et} \qquad \bar{\lambda}(S) = \bar{\lambda}(S_p) + \sum_v' 1 .$$

Preuve. — Il suffit de passer à la limite projective sur les suites exactes de 4.3 correspondant aux étages K_n de la tour cyclotomique. Q.E.D.

Nous terminons cette section par des critères de nullité de certains invariants d'Iwasawa.

4.6. PROPOSITION. — *On suppose que* k *vérifie la conjecture de Leopoldt. Soit* W *l'image de* $\prod_{v \in \Sigma} \mu(k_v)$ *dans* $\mathcal{O}_k$. *On a l'égalité :*

$$\dim T_k[p] = \dim (W \cap p\mathcal{O}_k / pW) + \dim \mathrm{Hom}\,(C\ell_S(K), \mu_p)^\Delta$$

(notations de 1.2). *Si* $p \neq 2$ *et si* $K = k(\mu_p)$ *est un corps* CM *on a :*

$$\dim T_k[p]^+ = \dim (W \cap p\mathcal{O}_k / pW)^+ + \dim C\ell_S(K)^-[p]$$

et

$$\dim T_k[p]^- = \dim (W \cap p\mathcal{O}_k / pW)^- + \dim C\ell_S(K)^+[p] .$$

Preuve. — De la suite exacte $0 \to W \to \mathcal{O}_k \to T_k \to 0$ on tire, par le lemme du serpent, la suite exacte

$$\cdots \to W/pW \to \mathcal{O}_k/p\mathcal{O}_k \to T_k/pT_k \to 0 .$$

On conclut en appliquant 1.2.

4.7. COROLLAIRE. — *Supposons que* $p \neq 2$ *et que* K *est un corps* CM *vérifiant la conjecture de Leopoldt. Alors :*

i) $X_\infty'^+ = (0)$ *si et seulement si* $C\ell_S(K)^+ = (0) = (W \cap p\mathcal{O}_K / p\mathcal{O}_K)^-$ (comparer à 2.5).

ii) $\lambda'^- = \mu'^- = 0$ *si et seulement si*

$$C\ell_S(K)^- = (0) = (W \cap p\mathcal{O}_K / p\mathcal{O}_K)^+ .$$

Preuve. — Comme $A'_\infty(1)^\Gamma \simeq T_K$, on en déduit que $A'^+_\infty(1)^\Gamma \simeq T_K^-$ et $A'^-_\infty(1)^\Gamma \simeq T_K^+$. La nullité de X'^+_∞ équivaut à celle de $A'^+_\infty(1)^\Gamma$.

Comme X'^{-}_{∞} n'a pas de sous-module fini non nul, la nullité simultanée de λ'^{-} et u'^{-} équivaut à la nullité de X'^{-}_{∞}, donc à celle de $A'^{-}_{\infty}(1)^{\Gamma}$. Q.E.D.

4.8. *Remarque.* — Si k contient μ_p, Kramer et Candiotti [15] montrent que le produit des symboles de Hilbert induit une dualité entre $W + pX_k/pX_k$ et $R_2k[p]/H_2k[p]$. Voir aussi le § 5.

5. $\mathcal{C}_k$, T_k et K_2.

Pour étudier la K-théorie des corps de nombres algébriques, le cadre idoine est celui de la cohomologie étale, ainsi qu'il est montré par exemple dans [22]. Cependant, si l'on se limite au K_2, la cohomologie galoisienne suffit (au prix parfois de quelques longueurs). Tate [23] a montré que $K_2k\{p\}$, la partie p-primaire de K_2k, est canoniquement isomorphe au groupe de cohomologie p-adique $H^2(\mathcal{G}, \mathbf{Z}_p(2))_{\text{tor}}$, où $\mathcal{G}$ est le groupe de Galois absolu de k. Dans l'esprit de [23] et des sections précédentes, nous voulons montrer le résultat principal suivant :

5.1. THÉORÈME. — *Soit O_S l'anneau des S-entiers de k. La partie p-primaire $K_2O_S\{p\}$ est canoniquement isomorphe au groupe de cohomologie p-adique $H^2(\mathcal{G}_S, \mathbf{Z}_p(2))$. En particulier, ce groupe de cohomologie est fini.*

(Pour une démonstration « étale », voir Lichtenbaum [16] ou Soulé [22].)

La démonstration va se faire en identifiant K_2O_S à un noyau modéré. Par définition, *le noyau modéré* R_2k (resp. *le noyau hilbertien* H_2k) est l'intersection des noyaux des symboles modérés (resp. hilbertiens). On sait, d'après Quillen, que $K_2O \simeq R_2k$, où O est l'anneau des entiers de k. Plus généralement, on sait que K_2O_S est isomorphe à un noyau S-modéré. Plus précisément, on a une suite exacte :

$$0 \to K_2O_S \to K_2k \xrightarrow{m_s} \bigoplus_{v \notin S} k(v)^* \to 0,$$

où m_S est le produit des symboles modérés pour $v \notin S$, et $k(v)$ est le corps résiduel en v ([23], § 5). On sait que $K_2O\{p\} = K_2O_S\{p\}$.

Preuve du théorème. — Puisque le groupe $\Delta = \text{Gal}(k(\mu_p)/k)$ est d'ordre premier à p, une procédure de réduction standard permet de se ramener au cas où $\mu_p \subset k$.

Soient alors $k_S(p)$ et G_S comme dans l'introduction, $k(p)$ la pro-p-extension maximale de k, $G = \mathrm{Gal}(k(p)/k)$. Comme $k_S(p)$ contient μ_{p^∞}, on montre comme dans [12], 6.3, que

$$H^n(\mathcal{G}_S, \mathbf{Q}_p/\mathbf{Z}_p(i)) \simeq H^n(G_S, \mathbf{Q}_p/\mathbf{Z}_p(i))$$

et

$$H^n(\mathcal{G}, \mathbf{Q}_p/\mathbf{Z}_p(i)) \simeq H^n(G, \mathbf{Q}_p/\mathbf{Z}_p(i))$$

pour tous entiers n et i. La clé de la démonstration du théorème va être le calcul des groupes $H^n(G_S, \mathbf{Q}_p/\mathbf{Z}_p(2))$, $n = 1,2$. Par inflation-restriction, on a la suite exacte :

$$0 \to H^1(G_S, \mathbf{Q}_p/\mathbf{Z}_p(2)) \to H^1(G, \mathbf{Q}_p/\mathbf{Z}_p(2)) \to H^1(k(p)/k_S(p), \mathbf{Q}_p/\mathbf{Z}_p(2))^{G_S} \to H^2(G_S, \mathbf{Q}_p/\mathbf{Z}_p(2)) \to H^2(G, \mathbf{Q}_p/\mathbf{Z}_p(2)) \to \cdots.$$

On sait que $H^2(G, \mathbf{Q}_p/\mathbf{Z}_p(2)) = 0$ ([21], II.11) et $H^2(G_S, \mathbf{Q}_p/\mathbf{Z}_p(2)) = 0$ d'après [24] (c'est l'analogue en K-théorie de la conjecture de Leopoldt). Il reste à calculer $H^1(k(p)/k_S(p), \mathbf{Q}_p/\mathbf{Z}_p(2))^{G_S}$.

Soit U un ensemble quelconque de places contenant S. D'après le théorème d'O. Neumann [18], $\mathrm{Gal}(k_U(p)/k_S(p))$ est isomorphe à un produit pro-p-libre $\underset{v \in U-S}{*} I_v$, où I_v est engendré par les groupes d'inertie des places v_2 de $k_U(p)$ divisant les places v_1 de $k_S(p)$ au-dessus de v. Ces groupes d'inertie sont isomorphes à $\mathbf{Z}_p$ ou $\{0\}$ suivant que k_v contient ou non μ_p. Leur cohomologie est facile à calculer : soient T_v la $\mathbf{Z}_p$-extension non ramifiée de k_v, $k_v(p)$ sa pro-p-extension maximale; alors $H^1(k_v(p)/T_v, \mu_{p^\infty}(2)) \simeq T_v^* \otimes \mu_{p^\infty}$ (voir [21]). Or le $\mathrm{Gal}(k_v(p)/T_v)$-module $T_v^* \otimes \mu_{p^\infty}$ est isomorphe au $\mathrm{Gal}(\overline{k(v)}/k(v))$-module μ_{p^∞}.

En prenant pour U l'ensemble des places de k, on obtient une suite exacte :

$$0 \to H^1(G_S, \mathbf{Q}_p/\mathbf{Z}_p(2)) \to H^1(G, \mathbf{Q}_p/\mathbf{Z}_p(2)) \to \bigoplus_{v \notin S} \mu(k(v)) \to H^2(G_S, \mathbf{Q}_p/\mathbf{Z}_p(2)) = 0.$$

Comme $\bigoplus_{v \notin S} \mu(k_v)$ est de torsion, on en déduit une autre suite exacte :

$$0 \to H^1(G_S, \mathbf{Q}_p/\mathbf{Z}_p(2))/\mathrm{div} \to H^1(G, \mathbf{Q}_p/\mathbf{Z}_p(2))/\mathrm{div} \to \bigoplus_{v \notin S} \mu(k(v)) \to 1,$$

où A/div désigne le quotient A/A_{div}.

Or $H^1(G,\mathbf{Q}_p/\mathbf{Z}_p(2))/\text{div} \simeq H^2(G,\mathbf{Z}_p(2))_{\text{tor}}$ ([23], § 2) $\simeq K_2k\{p\}$, et la comparaison avec la définition de K_2O_S montre immédiatement que $K_2O_S\{p\} \simeq H^1(G_S,\mathbf{Q}_p/\mathbf{Z}_p(2))/\text{div}$. Comme c'est un groupe fini, on a bien l'isomorphisme cherché $K_2O_S\{p\} \simeq H^2(G_S,\mathbf{Z}_p(2))$. Q.E.D.

5.2. COROLLAIRE. — *Pour tout entier q égal à une puissance de p, on a un isomorphisme canonique $K_2O_S/qK_2O_S \simeq H^2(\mathscr{G}_S,\mu_q(2))$. Si k contient μ_q, cet isomorphisme induit une dualité parfaite*

$$\text{Ш}_k(S)[q] \times (K_2O_S/qK_2O_S)(-1) \to \mu_q$$

(cette dualité est l'analogue au niveau fini du théorème 4 de Coates [5]; pour $q = p$, c'est la « mauvaise dualité » de Kramer-Candiotti [15]).

Preuve. — Cela résulte immédiatement du théorème, de la suite exacte $1 \to \mu_q(2) \to \mathbf{Q}_p/\mathbf{Z}_p(2) \to \mathbf{Q}_p/\mathbf{Z}_p(2) \to 0$ et la nullité de $H^2(\mathscr{G}_S,\mathbf{Q}_p/\mathbf{Z}_p(2))$. Q.E.D.

Dans l'optique d'une « théorie de Galois » pour K_2O_S, signalons le critère de nullité suivant qui fait intervenir les co-invariants :

5.3. COROLLAIRE (comparer à 1.4). — *Soit L/k une extension galoisienne finie contenue dans $k_S(p)/k$, de groupe de Galois G. Alors $(K_2O_S(L)\{p\})_G \simeq K_2O_S(k)\{p\}$. En particulier, $K_2O_S(L)\{p\} = (0)$ si et seulement si $K_2O_S(k)\{p\} = (0)$.*

Preuve. — Choisissons q suffisamment grand pour que

$$K_2O_S(L)\{p\} \simeq H^2(\mathscr{G}_S(L),\mu_q(2)) \quad \text{et} \quad K_2O_S(k)\{p\} \simeq H^2(\mathscr{G}_S(k),\mu_q(2)).$$

Nous pouvons alors faire intervenir le module dualisant pour montrer, comme dans 1.6, que $(K_2O_S(L)\{p\}^*)^G \simeq K_2O_S(k)\{p\}^*$. Q.E.D.

5.4. COROLLAIRE. — *Soit Y_∞ le groupe de Galois de la pro-p-extension abélienne S-ramifiée maximale de K_∞. On a un isomorphisme canonique : $K_2O_S\{p\}^* \simeq t_{\mathbf{Z}_p}(Y_\infty(-2)_{G_\infty})$, où $t_{\mathbf{Z}_p}(.)$ désigne la $\mathbf{Z}_p$-torsion.*

(Cela donne une « formule analytique » pour $|K_2O_S\{p\}|$ puisque $Y_\infty(-2)^{G_\infty} = (0)$ d'après [24]; pour $S = S_p$ et k totalement réel, c'est le théorème 13 de Coates [4] et la conjecture de Birch-Tate.)

Preuve. — On a vu que $K_2O_S\{p\} \simeq H^1(\mathscr{G}_S,\mathbf{Q}_p/\mathbf{Z}_p(2))/\text{div}$. Comme $H^i(G_\infty,\mathbf{Q}_p/\mathbf{Z}_p(2)) = 0$ pour $i = 1,2$ (voir [24]), l'inflation-restriction

montre que

$$H^1(\mathcal{G}_S, \mathbf{Q}_p/\mathbf{Z}_p(2)) \simeq H^1(k_S/K_\infty, \mathbf{Q}_p/\mathbf{Z}_p(2))^{G_\infty}.$$

Par dualité, on obtient bien un isomorphisme

$$K_2O_S\{p\}^* \simeq t_{\mathbf{Z}_p}(Y_\infty(-2)_{G_\infty}). \qquad \text{Q.E.D.}$$

5.5. *Remarque.* — On notera l'analogie entre $K_2O_S\{p\}^*$ et $\mathcal{C}_k(S)$. Le module $\mathcal{C}_k$ est la $\mathbf{Z}_p$-torsion de $(Y_\infty)_{G_\infty}$ et, si k vérifie la conjecture de Leopoldt, $\mathcal{C}_k^*$ est isomorphe au groupe de cohomologie p-adique

$$H^2(\mathcal{G}_S, \mathbf{Z}_p) = \varprojlim_n H^2(\mathcal{G}_S, \mathbf{Z}/p^n\mathbf{Z}).$$

La même analogie existe entre T_k et le dual $H_2k\{p\}^*$ du noyau hilbertien.

5.6. THÉORÈME. — *On a un isomorphisme*

$$H_2k\{p\}^* = \mathrm{Ker}^2_{S_p}(\mathbf{Q}_p/\mathbf{Z}_p(-1)).$$

Si k contient μ_q (q est une puissante de p), on a une dualité parfaite :

$$T_k[q] \times (H_2k/qH_2k)(-1) \to \mu_q.$$

Preuve. — Par définition, on a une suite exacte

$$0 \to H_2k\{p\} \to R_2k\{p\} \to \prod_{v|p} \mu(k_v).$$

De la description de $R_2k\{p\}$ donnée en 5.1, il résulte immédiatement que

$$H_2k\{p\} \simeq \mathrm{Ker}^2_S(\mathbf{Z}_p(2)) = \varprojlim_n \mathrm{Ker}^2_{S_p}(\mathbf{Z}/p^n\mathbf{Z}(2)).$$

Or d'après la dualité globale de Poitou-Tate ([12], 1.3), $\mathrm{Ker}^2_{S_p}(\mathbf{Z}_p(2))$ est dual de $\mathrm{Ker}^1_{S_p}(\mathbf{Q}_p/\mathbf{Z}_p(-1))$. Le reste est immédat. Q.E.D.

5.7. COROLLAIRE (voir aussi [15], corollaire 3.3). — *Si k contient μ_p, on a l'égalité :*

$$\dim H_2K/pH_2K = \dim C\ell_{S_p}(K)[p] + \dim (W \cap p\mathcal{C}_K/pW).$$

Preuve. — C'est immédiat, à partir de 5.7 et 4.5. Q.E.D.

Des applications au problème de plongement dans les $\mathbf{Z}_p$-extensions seront données dans un article ultérieur.

BIBLIOGRAPHIE

[1] H. BASS, éd., « Algebraic K-theory II », *Springer Lect. Notes in Math.*, n° 342 (1973).

[2] F. BERTRANDIAS et J.-J. PAYAN, Γ-extensions et invariants cyclotomiques, *Ann. Sci. ENS*, 5 (1972), 517-543.

[3] J. COATES, *p*-adic L-functions and Iwasawa's theory, dans « Algebraic Number Fields », *Proc. Sympos. Durham*, Academic Press (1977).

[4] J. COATES, K-theory and Iwasawa's analogue of the Jacobian, dans « Algebraic K-theory II », *Springer Lect. Notes in Math.*, n° 342 (1973).

[5] J. COATES, On K_2 and some classical conjectures in algebraic number theory, *Ann. of Math.*, 95 (1972), 99-116.

[6] A. FRÖHLICH, éd., « Algebraic Number Fields », *Proc. Sympos. Durham*, Academic Press (1977).

[7] R. GILLARD, Formulations de la conjecture de Leopoldt et étude d'une condition suffisante, *Abh. Math. Sem. Hamburg*, 48 (1979), 125-138.

[8] G. GRAS, Groupe de Galois de la *p*-extension abélienne *p*-ramifiée maximale d'un corps de nombres, *J. reine angew. Math.*, 333 (1982), 82-132.

[9] G. GRAS, Logarithme *p*-adique et groupes de Galois, *J. reine angew. Math.*, 343 (1983), 64-80.

[10] G. GRAS, Sur les Z_2-extensions d'un corps quadratique imaginaire, *Ann. Inst. Fourier*, 33-4 (1983), 1-18.

[11] R. GREENBERG, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.*, 98 (1976), 263-284.

[12] K. HABERLAND, « Galois cohomology of algebraic number fields », *Deutscher Verlag der Wissen.*, Berlin (1978).

[13] K. IWASAWA, On Z_ℓ-extensions of algebraic number fields, *Ann. Math.*, 98 (1973), 246-326.

[14] J.-F. JAULENT, Théorie de Kummer et K_2 des corps de nombres, prépublication.

[15] K. KRAMMER et A. CANDIOTTI, On K_2 and Z_ℓ-extensions of number fields, *Amer. J. Math.*, 100-1 (1978), 177-196.

[16] S. LICHTENBAUM, Values of zeta functions, étale cohomology and algebraic K-theory, dans « Algebraic K-theory II », *Springer Lect. Notes in Math.*, n° 342 (1973).

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

[18] O. NEUMANN, On *p*-closed number fields and an analogue of Riemann's existence theorem, dans « Algebraic Number Fields », *Proc. Sympos. Durham*, Academic Press (1977).

[19] T. NGUYEN-QUANG-DO, Sur la structure galosienne des corps locaux et la théorie d'Iwasawa, *Compos. Math.*, 46, 1 (1982), 85-119.

[20] T. NGUYEN-QUANG-DO, Résidu en $s = 1$ de certaines fonctions d'Iwasawa, Groupe d'Étude Analyse Ultra-métrique, Mars 1984.

[21] J.-P. SERRE, « Cohomologie galoisienne », *Springer Lect. Notes in Math.*, *n°* 5 (1964).

[22] C. SOULÉ, K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale, *Invent. Math.*, 55,3(1979), 251-295.
[23] J. TATE, Relations between K_2 and Galois cohomology, *Invent. Math.*, 36 (1976), 257-274.
[24] J. TATE, Letter to Iwasawa, dans « Algebraic K-theory II », *Springer Lect. Notes in Math.*, n° 342 (1973).
[25] K. WINGBERG, Duality theorems for Γ-extensions of algebraic number fields, à paraître dans *Compos. Math.*

Manuscrit reçu le 4 mars 1985
révisé le 11 juin 1985.

Thong NGUYEN-QUANG-DO,
Université de Paris VII
UER de Mathématique-Informatique
LA 212 au CNRS
2, place Jussieu
75251 Paris Cedex 05.