Publ. Mat. **46** (2002), 201–219

SUR LE RANG D'UNE EXTENSION PRO-p-LIBRE D'UN CORPS DE NOMBRES

Arthur Lannuzel

Abstract

For an algebraic number field k and a prime number p (if $p = 2$, we assume that $\mu_4 \subset k$), we study the maximal rank ρ_k of a free pro-p-extension of k. We give various interpretations of $1+r_2(k)-\rho_k$. The first uses Iwasawa theory, the second uses the envelope of a module and the third is local-global. These expressions confirm that $1 + r_2 - \rho_k$ is related to the torsion of a certain Iwasawa module, hence to the dualizing module of a certain Galois group (under Leopoldt's conjecture).

Introduction

Soit k un corps de nombres algébriques (*i.e.* une extension finie de $\mathbb{Q}$) et p un nombre premier fixé (si $p = 2$, on impose de plus $\mu_4 \subset k$). Soit S un ensemble fini de places de k contenant S_p, l'ensemble des places divisant p, et $G_S(k)$ le groupe de Galois de la pro-p-extension maximale S-ramifiée k_S de k (*i.e.* non-ramifiée en dehors des places de S).

Les propriétés p-adiques de k se reflètent dans la structure du groupe de Galois $G_S(k)$, qui peut être considéré comme un analogue p-adique du groupe fondamental d'un courbe de genre g.

Le cas le plus simple est celui de genre 0, dont l'analogue p-adique est fourni par les corps dits "p-rationnels" ([**MN**], [**GJ**]), *i.e.* ceux pour lesquels $G_{S_p}(k)$ est un pro-p-groupe libre. L'étape naturelle suivante est d'étudier les quotients pro-p-libres d'un $G_{S_p}(k)$.

Convenons d'appeler F_d-extension de k une extension L_d de k telle que $\mathrm{Gal}(L_d/k)$ soit un pro-p-groupe libre à d générateurs (de façon générale, F_d désignera toujours un pro-p-groupe libre à d générateurs). Une telle extension sera dite pro-p-libre; on parlera aussi de pro-p-extension libre.

2000 *Mathematics Subject Classification.* 11R23, 11R32, 11R34.
Mots-clés. Extensions pro-p-libres, pro-p-extensions libres, corps de nombres.

Comme une F_d-extension est S_p-ramifiée (*cf.* [**Y1**]), le problème précédent revient à étudier l'entier

$$\rho_k = \max\{d \in \mathbb{N} \text{ tel que } k \text{ admette une } F_d\text{-extension}\}.$$

L'invariant ρ_k a déjà été étudié par différents auteurs, en particulier M. Yamagishi ([**Y1**], [**Y2**]), K. Wingberg ([**W1**] et [**W2**]), T. Nguyen Quang Do ([**N1**]). Il est relié à certains problèmes de structure galoisienne (*cf.* Sections 2 et 3). Dans la suite, on prêtera une attention particulière à la différence $r_2(k)+1-\rho_k$ où $r_2(k)$ désigne le nombre de places complexes de k. En effet, si $\tilde{K}$ est la composée de toutes les $\mathbb{Z}_p$-extensions de k, alors $\tilde{\Gamma} := \mathrm{Gal}(\tilde{K}/k) \cong \mathbb{Z}_p^{r_2(k)+1+\delta_p(k)}$, où $\delta_p(k)$ est un entier naturel, conjecturalement nul (Leopoldt). On en déduit immédiatement que $\rho_k \leq r_2(k) + 1$ sous la conjecture de Leopoldt.

La conjecture précédente en p est équivalente à supposer $\mathrm{H}^2(\mathrm{Gal}(k_S/k), \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Elle est démontrée pour toute extension abélienne finie de $\mathbb{Q}$, et si elle est vraie pour L en p, elle est vraie pour toute sous-extension de L en p. Par extension, on appelle conjecture généralisée de Leopoldt pour une extension L/k infinie en p, l'hypothèse $\mathrm{H}^2(\mathrm{Gal}(k_S/L), \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Si L contient la $\mathbb{Z}_p$-extension cyclotomique de k, la conjecture faible est vraie pour L en p. De plus, pour une tour d'extensions $L/k/\mathbb{Q}$ où $L/\mathbb{Q}$ est infinie et $k/\mathbb{Q}$ est finie, la conjecture forte pour k en p entraîne la conjecture faible pour L en p.

Si k est totalement réel ($r_2 = 0$), il est clair que $\rho_k = 1$, mais, si k est imaginaire ($r_2 \neq 0$), le problème est beaucoup plus compliqué et relié à des propriétés arithmétiques intéressantes de k. Par ailleurs, on connaît des exemples (*cf.* [**Y1**]) où $\rho_k < r_2 + 1$. La relation entre les hypothèses '$\rho_k = r_2 + 1$' et 'k est un corps p-rationnel' est étudiée dans [**LN**] en relation avec certaines conjectures dues à Greenberg en théorie d'Iwasawa des $\mathbb{Z}_p$-extensions multiples.

Dans cet article, guidé par le cas local, nous allons mettre en place des bornes de la différence $r_2(k) + 1 - \rho_k$. La première borne provient de résultats de structure galoisienne démontrés dans [**LN**] , la deuxième de la théorie de l'enveloppe d'un module (*cf.* [**J**] et [**GW**]), la troisième utilisera des méthodes locales-globales. Chacune de ces expressions nous donnera des conditions pour avoir l'égalité $\rho_k = r_2(k) + 1$. Ces expressions nous permettent de constater que la différence $1 + r_2 - \rho_k$ est relié au foncteur $\mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(\bullet)$ (*cf.* notations ci-dessous), donc au module dualisant sous la conjecture de Leopoldt.

Remerciements. Ce travail a été réalisé au Laboratoire de Mathématiques de l'Université de Besançon et au Départament de Matemàtiques de la Universitat Autònoma de Barcelona. Je remercie ces deux institutions, ainsi que Thong Nguyen Quang Do dont les conseils et les suggestions m'ont permis de mener ce travail à bien.

Notations

Pour un pro-p-groupe G, on notera $d(G)$ et $r(G)$ son nombre minimal de générateurs et de relations respectivement. On sait que $d(G) = \dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p)$ et $r(G) = \dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathbb{F}_p)$.

Avec l'hypothèse sur p, on sait que $\mathrm{cd}(G_S) \leq 2$ et $\chi(G_S(k)) := \sum_{i=0}^{\infty}(-1)^{i+1} \dim_{\mathbb{F}_p} \mathrm{H}^i(G_S(k), \mathbb{F}_p) = r_2(k)$ où $\chi(\cdot)$ désigne la caractéristique d'Euler-Poincaré (voir e.g. [**Ha**]).

Pour une place v de k, on note $G_v = G_v(k)$, le groupe de décomposition de $G_S(k)$ pour une place choisie de k_S au-dessus de v et $\mathcal{G}_v$ le pro-p-groupe de Galois absolue du localisé k_v de k.

μ_{p^s} avec $s \in \mathbb{N}$ désigne l'ensemble des racines de l'unité d'ordre p^s et $\mu_{p^\infty} := \cup_{n\in\mathbb{N}}\mu_{p^s}$.

$(\cdot)^{ab}$ désigne l'abélianisé si l'argument est un groupe, le corps fixé par les commutateurs si l'argument est un corps.

$\mathfrak{X}_S(k) := (G_S(k))^{ab}$. On réservera la notation $\mathfrak{X}(k)$ au cas $S = S_p$.

Une $\mathbb{Z}_p$-extension multiple de rang a (ou $\mathbb{Z}_p^a$-extension) de k sera notée $K^{(a)}$, $\Gamma^{(a)} := \mathrm{Gal}(K^{(a)}/k) \cong \mathbb{Z}_p^a$.

Soit $\Lambda_a = \mathbb{Z}_p[[\Gamma^{(a)}]]$. On sait que $\Lambda_a \cong \mathbb{Z}_p[[T_1, \ldots, T_a]]$, l'algèbre commutative des séries formelles à a indéterminées. La notation Λ sera reservé au cas $a = 1$.

Pour une $\mathbb{Z}_p^a$-extension $K^{(a)}/k$, le Λ_a-module $\mathfrak{X}_S(K^{(a)}) := \mathrm{Gal}(k_S/K^{(a)})^{ab}$ sera noté en abrégé $\mathfrak{X}_S^{(a)}$ (ou $\mathfrak{X}^{(a)}$ si $S = S_p$).

Pour $K^{(a)}/k$ fixée, on prend une famille d'extensions finies $(k_n/k)_{n\in\mathbb{N}}$ telle que $K^{(a)} = \varinjlim_n k_n$ et donc $\mathfrak{X}^{(a)} = \varprojlim_n \mathfrak{X}(k_n)$. On note Γ_n le groupe de Galois de $K^{(a)}/k_n$.

Pour tout R anneau commutatif intègre, pour tout R-module M, on notera $\mathrm{Tor}_R\, M$ la R-torsion de M et $\mathrm{fr}_R\, M$ le quotient de M par sa R-torsion.

1. Rappels concernant le cas local

Les résultats suivants montrent que le problème est résolu dans le cas où k est un corps local (*cf.* [**JW**], [**N1**], [**N4**]). Nous rappelons ces résultats pour donner une idée du type de résultats recherchés.

Théorème 1.1 ([**N1**]). *Si $k/\mathbb{Q}_p$ est irrégulier (*i.e. *il existe $s \geq 1$ tel que $\mu_{p^s} \subset k$) et K/k est une extension galoisienne de groupe de Galois H, les assertions suivantes sont équivalentes:*

(i) *K/k se plonge dans une F_d-extension, où F_d est le pro-p-groupe libre à d générateurs.*
(ii) *Tout problème de plongement $\{1\} \to N \to E \to H \to \{1\}$, où N est un p-groupe tel que $d(E) = d(H)$, possède une solution.*
(iii) *$\mathfrak{X}(K) \cong R^{ab}_{d(H)}(H) \times \mathbb{Z}_p[H]^{n+2-2d(H)-\delta} \times M_K$, où M_K est un $\mathbb{Z}_p[H]$-module cohomologiquement trivial et indécomposable, $\delta = 1$ si $\mu_{p^\infty}(K) \subset N_{\mathrm{Gal}(K/k)}(K^*) \cdot K^{*p}$, 0 sinon. $R^{ab}_{d(H)}(H)$ désigne le module des relations de H dans une présentation libre de rang $d(H)$ de H.*

Remarque 1.2 ([**N1**]). Puisque dans le cas régulier le groupe de Galois de la pro-p-extension maximale est libre, on en déduit sans problème que dans le cas local irrégulier, $\rho_k = \frac{[k:\mathbb{Q}_p]}{2} + 1$ et dans le cas local régulier, $\rho_k = [k : \mathbb{Q}_p] + 1$.

Question 1.3. *Y a-t-il un analogue à ce théorème dans le cas global?*

Le module M_K de (iii) est une enveloppe (*cf.* [**N4**]) de $\mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}(K) = \mu_{p^\infty}(K)$ (*i.e.* on a une suite exacte $\{0\} \to \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}(K) \to M_K \to N \to \{0\}$ avec M_K cohomologiquement trivial et N $\mathbb{Z}_p$-libre). On peut en donner une description cohomologique. Le résultat suivant est démontré dans [**N4**] et utilise le fait que l'on connaisse la torsion $\mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}(K)$.

Théorème 1.4 ([**N4**]). *Soit K/k une extension de groupe de Galois H. Avec les notations du théorème précédent, si K/k se plonge dans une $F_{d(H)}$-extension cyclotomique $L_{d(H)}/k$ (*i.e. *$\mu_{p^\infty} \subset L_{d(H)}$) alors*

$$M_K \cong \mathrm{H}^1(\mathrm{Gal}(L_{d(H)}/K), \mathbb{Z}_p(1)).$$

2. Expression de $(1 + r_2) - \rho_k$ comme rang d'un module d'Iwasawa

On va maintenant s'intéresser à des problèmes de structure galoisienne dans le cas global. Ces résultats sont démontrés dans [**LN**]. Ils permettent de comprendre l'hypothèse '$\rho_k = r_2 + 1$'.

Soit $L := L_\rho$ une extension pro-p-libre de k de rang ρ. D'après [**Y1**], on sait que l'extension L/k est non-ramifiée en dehors de p, donc $L \subset k_S$.

Soit K une pro-p-extension de k incluse dans L. Posons $R := \mathrm{Gal}(L/K)$ et $H := \mathrm{Gal}(K/k)$.

On a la suite exacte

$$\{1\} \longrightarrow \mathrm{Gal}(k_S/L) \longrightarrow \mathrm{Gal}(k_S/K) \longrightarrow R \longrightarrow \{1\}.$$

La suite d'inflation-restriction nous donne alors la suite exacte

$$\{0\} \longrightarrow H^1(R, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(\mathrm{Gal}(k_S/K), \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(\mathrm{Gal}(k_S/L), \mathbb{Q}_p/\mathbb{Z}_p)^R \longrightarrow \{0\},$$

puisque R est un pro-p-groupe libre en tant que sous-groupe fermé d'un pro-p-groupe libre.

Ainsi, en dualisant (Pontrjagin), on obtient:

$$\{0\} \longrightarrow \mathfrak{X}_S(L)_R \longrightarrow \mathfrak{X}_S(K) \longrightarrow R_\rho^{ab}(H) \longrightarrow \{0\} \tag{1}$$

où l'on a posé $R_\rho^{ab}(H) := R^{ab}$ qui est le module des relations dans la présentation libre de rang ρ de H donnée par:

$$\{1\} \longrightarrow R \longrightarrow \mathrm{Gal}(L/k) \longrightarrow H \longrightarrow \{1\}.$$

Rappelons que le "module des relations" $R_\rho^{ab}(G)$ peut être défini pour n'importe quel pro-p-groupe G qui est quotient du pro-p-groupe F_ρ, et qu'il apparaît dans la résolution de Lyndon (*cf.* e.g. [**N1**]),

$$\{0\} \longrightarrow R_\rho^{ab}(G) \longrightarrow \mathbb{Z}_p[[G]]^\rho \longrightarrow \mathbb{Z}_p[[G]] \longrightarrow \mathbb{Z}_p \longrightarrow 0.$$

Voici l'analogue global du Théorème 1.1(iii):

Théorème 2.1. *Soit L_ρ une pro-p-extension libre de k de rang ρ, contenant une sous-extension galoisienne K/k de groupe de Galois H. Posons $R := \mathrm{Gal}(L_\rho/K)$.*

Si toute sous-extension finie de K/k vérifie la conjecture de Leopoldt en p, alors

$$\mathfrak{X}_S(L_\rho)_R \oplus \mathbb{Z}_p[[H]]^{\rho-d(H)} \oplus R_{d(H)}^{ab}(H) \cong \mathfrak{X}_S(K).$$

Remarque 2.2. $\mathfrak{X}_S(L_\rho)_R$ est cohomologiquement trivial sous Leopoldt (voir par exemple la Proposition 3.4 ci-dessous), mais on n'en a pas de description analogue au Théorème 1.4. Voir cependant le paragraphe 3.

Preuve du théorème: Cf. [**LN**].

Corollaire 2.3. *Soit K/k une extension galoisienne finie de groupe de Galois H. On suppose que K vérifie la conjecture de Leopoldt en p. Si K/k se plonge dans une F_{r_2+1}-extension, alors* $\mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K)$ *est un $\mathbb{Z}_p[H]$-module cohomologiquement trivial.*

Preuve: Dans cette situation, la proposition précédente montre que l'on a l'isomorphisme

$$\mathfrak{X}_S(L_{r_2+1})_{\mathrm{Gal}(F_{r_2+1}/K)} \cong \mathrm{Tor}_{\mathbb{Z}_p}\, \mathfrak{X}_S(K).$$

Or $\mathfrak{X}_S(L_{r_2+1})_{\mathrm{Gal}(F_{r_2+1}/K)}$ est cohomologiquement trivial sous Leopoldt. D'où le résultat. □

Remarque 2.4. Les relations qui apparaissent avec le module $\mathrm{Tor}_{\mathbb{Z}_p}\mathfrak{X}_S(K)$ peuvent être vues comme relations avec le module dualisant, $I_2(G_S(k))$. En effet, on sait que, sous la conjecture de Leopoldt pour toute sous-extension finie de k_S, $\varinjlim_n \mathrm{Tor}_{\mathbb{Z}_p}\, \mathfrak{X}_S(k_n) \cong I_2(G_S(k))$ avec $\cup_{n\in\mathbb{N}} k_n = k_S$ et $\mathrm{Tor}_{\mathbb{Z}_p}\, \mathfrak{X}_S(K) \cong I_2(G_S(k))^{G_S(K)}$ (*cf.* [**W1**]).

Si l'on applique ce qui précède au cas particulier des $\mathbb{Z}_p$-extensions multiples, on obtient le résultat suivant, démontré dans [**LN**]:

Proposition 2.5. *Soit L_ρ une pro-p-extension libre de k de rang ρ, contenant une $\mathbb{Z}_p^a$-extension $K^{(a)}$ ($a \le \rho$). On pose $R := \mathrm{Gal}(L_\rho/K^{(a)})$, $\Gamma^{(a)} := \mathrm{Gal}(K^{(a)}/k)$ et $\Lambda_a := \mathbb{Z}_p[[\Gamma^{(a)}]]$.*

*Si $K^{(a)}$ vérifie la conjecture de Leopoldt faible en p (*i.e. $\mathrm{H}^2(\mathrm{Gal}(k_S/K^{(a)}), \mathbb{Q}_p/\mathbb{Z}_p) = 0$*), le Λ_a-rang de $\mathfrak{X}_S(L_\rho)_R$ est égal à $r_2 + 1 - \rho$. En particulier $\rho = r_2 + 1$ si et seulement si $\mathfrak{X}_S(L_\rho)_{\mathrm{Gal}(L_\rho/K^{(a)})}$ est la Λ_a-torsion de $\mathfrak{X}_S(K^{(a)})$.*

Remarque 2.6. On retrouve le résultat connu suivant (*cf.* [**Y1**]): en supposant la conjecture faible de Leopoldt pour L_ρ^{ab}/k en p, on a $\rho_k \le r_2+1$.

3. $(1 + r_2) - \rho_k$ et l'enveloppe de $\mathfrak{X}_S(K)$

On va maintenant s'intéresser aux structures galoisiennes à "homotopie près" (*i.e.* à un facteur direct projectif près). Pour les généralités *cf.* [**J**].

Soit K/k une extension galoisienne de corps de nombres, de groupe de Galois H.

Soit M et N, des $\mathbb{Z}_p[[H]]$-modules. On dira que M est *homotope à* N, noté $M \sim N$, si il existe $a, b \in \mathbb{N}$ tels que $M \times \mathbb{Z}_p[[H]]^a \cong N \times \mathbb{Z}_p[[H]]^b$.

On dira que $g \in \mathrm{Hom}_{\mathbb{Z}_p[[H]]}(M, N)$ est *homotope à* 0, noté $g \sim 0$, si g se factorise à travers un $\mathbb{Z}_p[[H]]$-module projectif (donc libre car $\mathbb{Z}_p[[H]]$ est local). On pose alors

$$[M, N] := \mathrm{Hom}_{\mathbb{Z}_p[[H]]}(M, N)/\{g \sim 0\}.$$

Considérons la suite exacte d'augmentation appliquée à $G_S(k)$:

$$\{0\} \longrightarrow I(G_S(k)) \longrightarrow \mathbb{Z}_p[[G_S(k)]] \xrightarrow{\text{aug.}} \mathbb{Z}_p \longrightarrow 0.$$

Comme dans [**N2**], en appliquant l'homologie par rapport à $G_S(K)$ et en posant $\mathcal{Y}_S(K/k) := I(G_S(k))_{G_S(K)}$, on obtient la suite exacte:

$$\{0\} \longrightarrow \mathfrak{X}_S(K) \longrightarrow \mathcal{Y}_S(K/k) \longrightarrow I(H) \longrightarrow \{0\},$$

$I(H)$ étant l'idéal d'augmentation de H. Le module $\mathcal{Y}_S(K/k)$ est appelé l'*enveloppe* de $\mathfrak{X}_S(K)$, défini à homotopie près (*cf.* [**GW**]). Il est lié de façon étroite aux relations du groupe $G_S(K)$ par la matrice des dérivées de Fox (*cf.* e.g. [**N2**]). Il est cohomologiquement trivial si K vérifie Leopoldt.

La suite exacte précédente nous permet d'obtenir grâce à la résolution de Lyndon (*cf.* [**N1**]) le diagramme commutatif (push-out) suivant:

$$\begin{tikzcd}
\{0\} \arrow[r] & R^{ab}_{d(H)}(H) \arrow[r] \arrow[d] & \mathbb{Z}_p[[H]]^{d(H)} \arrow[r] \arrow[d, "\phi"] & I(H) \arrow[r] \arrow[d, equal] & \{0\} \\
\{0\} \arrow[r] & \mathfrak{X}_S(K) \arrow[r] & \mathcal{Y}_S(K/k) \arrow[r, "f_K"] & I(H) \arrow[r] & \{0\},
\end{tikzcd}$$

où ϕ est la flèche naturelle induite par la flèche correspondante dans la résolution de Lyndon pour $G_S(k)$.

On obtient ainsi de façon purement algébrique une suite exacte

$$(2)\quad \{0\} \longrightarrow R^{ab}_{d(H)}(H) \longrightarrow \mathfrak{X}_S(K) \oplus \mathbb{Z}_p[[H]]^{d(H)} \longrightarrow \mathcal{Y}_S(K/k) \longrightarrow \{0\}.$$

On a alors le théorème de caractérisation (*cf.* [**J**]) de $\mathfrak{X}_S(K)$ à homotopie près:

Théorème 3.1. *Soit k un corps de nombres algébriques, K/k une pro-p-extension de groupe de Galois H. A homotopie près, $\mathfrak{X}_S(K)$ est uniquement déterminé par les deux invariants suivants:*

(i) $\varinjlim_n \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(k_n)$ *où* $\varinjlim_n k_n = K$, k_n/k *finie.*

(ii) *La classe de f_K dans $[\mathcal{Y}_S(K/k), I(H)]$.*

Remarque 3.2. i) Il résulte directement de la définition de l'homotopie et du module $\mathcal{Y}_S(K/k)$ (*cf.* [**J**]) que $[\mathcal{Y}_S(K/k), I(H)] \cong \mathrm{H}^2(H, \varinjlim_n \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(k_n))^*$.

ii) De plus, dans le cas où H est fini et toute extension finie de k vérifie la conjecture de Leopoldt en p, la classe de f_K dans $[\mathcal{Y}_S(K/k), I(H)]$ correspond par l'isomorphisme précédent à l'image par la flèche naturelle de l'élément canonique $\mathrm{Id}_{I_2(G_S(k))} \in \mathrm{Hom}_{G_S(k)}(I_2(G_S(k)), I_2(G_S(k))) \cong \mathrm{H}^2(G_S(k), I_2(G_S(k)))^*$ dans $\mathrm{H}^2(H, \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K))^*$ (*cf.* [**J**, p. 190]).

Des cas particuliers intéressants consistent à éliminer l'un des deux invariants qui apparaissent dans le Théorème 3.1. A priori, on ne sait pas s'ils sont ou non indépendants. L'élimination de l'invariant (i) simplifie considérablement le problème: c'est l'étude de la p-rationalité qui est faite dans [**LN**]. La trivialité de l'invariant (ii) exprime un résultat de structure galoisienne:

Théorème 3.3. *Soit K/k une pro-p-extension de corps de nombres algébriques de groupe de Galois H. Les propositions suivantes sont équivalentes:*

(i) $f_K \sim 0$.
(ii) *La suite exacte* (2) *admet un relèvement (*i.e. $\mathfrak{X}_S(K) \sim \mathcal{Y}_S(K/k) \oplus R^{ab}_{d(H)}(H)$*).*
(iii) *Tout problème de plongement* $\{1\} \to N \to G \to H \to \{1\}$ *(suite exacte de p-groupes) avec N abélien et $d(G) = d(H)$ admet une solution.*

Preuve: (i)$\Leftrightarrow$(ii) découle de ce qui précède (*cf.* [**J**, p. 190]).

(i)$\Leftrightarrow$(iii). En prenant la cohomologie de la suite exacte

$$\{0\} \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K) \longrightarrow \mathcal{Y}_S(K/k) \longrightarrow \mathrm{fr}_{\mathbb{Z}_p} \mathcal{Y}_S(K/k) \longrightarrow \{0\},$$

on voit que $\mathrm{H}^2(H, \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K)) \cong \mathrm{H}^1(H, \mathrm{fr}_{\mathbb{Z}_p} \mathcal{Y}_S(K/k))$.

En prenant la cohomologie de la suite exacte

$$\{0\} \longrightarrow \mathfrak{X}_S(K) \longrightarrow \mathcal{Y}_S(K/k) \longrightarrow I(H) \longrightarrow \{0\},$$

on voit que $\mathrm{H}^2(H, \mathfrak{X}_S(K)) \cong \mathrm{H}^1(H, I(H))$.

Or $\mathrm{H}^1(H, \mathrm{fr}_{\mathbb{Z}_p} \mathcal{Y}_S(K/k)) \cong [I(H), \mathrm{fr}_{\mathbb{Z}_p} \mathcal{Y}_S(K/k)]$ et $\mathrm{H}^1(H, I(H)) \cong [I(H), I(H)]$ (*cf.* [**GW**]).

On obtient donc le diagramme commutatif:

$$\begin{array}{ccc} \mathrm{H}^2(H, \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K)) & \xrightarrow{\text{nat.}} & \mathrm{H}^2(H, \mathfrak{X}_S(K)) \\ \downarrow \cong & & \downarrow \cong \\ [I(H), \mathrm{fr}_{\mathbb{Z}_p} \mathcal{Y}_S(K/k)] & \xrightarrow{\hat{f}_K} & [I(H), I(H)]. \end{array}$$

On en déduit alors le résultat. □

Si l'on applique ce qui précède au cas des F_d-extensions, en prenant $K = L_{\rho_k}$, on obtient la suite exacte scindée:

$$\{0\} \longrightarrow \mathfrak{X}_S(L_{\rho_k}) \longrightarrow \mathcal{Y}_S(L_{\rho_k}/k) \longrightarrow \mathbb{Z}_p[[F_{\rho_k}]]^{\rho_k} \longrightarrow \{0\},$$

puisque $I(F_{\rho_k})$ est un $\mathbb{Z}_p[[F_{\rho_k}]]$-module libre de rang ρ_k (*cf.* [**Br**] ou directement à partir de la résolution de Lyndon).

On en déduit alors en prenant les co-invariants:

Proposition 3.4. *Soit K/k une extension finie de corps de nombres algébriques de groupe de Galois H telle que $K \subset L_{\rho_k}$. On suppose que K vérifie la conjecture de Leopoldt en p. Alors $f_K \sim 0$ et on a:*

$$\mathcal{Y}_S(K/k) \cong \mathbb{Z}_p[H]^{\rho_k} \oplus \mathfrak{X}_S(L_{\rho_k})_{R_{\rho_k}(H)}.$$

(Comparer à 2.1 et au résultat local 1.1.)

Théorème 3.5. i) *Soit K/k une extension finie de corps de nombres algébriques de groupe de Galois H telle que $K \subset L_{\rho_k}$. On suppose que K vérifie la conjecture de Leopoldt en p.*

On a:

$$m(\mathfrak{X}_S(K)) + \dim_{\mathbb{F}_p} \mathrm{H}^1(H, \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K))[p] \geq r_2(k) + 1 - \rho_k$$
$$\geq \dim_{\mathbb{F}_p} \mathrm{H}^1(H, \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K))[p],$$

où $m(\mathfrak{X}_S(K))$ est l'entier maximal m tel que $\mathfrak{X}_S(K)$ admette un facteur direct isomorphe à $\mathbb{Z}_p[H]^m$.

ii) *Dans le cas particulier où K est tel que $d(H) = \rho_k$ (par exemple si K est le sous corps de L_{ρ_k} fixé par $[F_{\rho_k}, F_{\rho_k}]F_{\rho_k}^p$), on a*

$$r_2(k) + 1 - \rho_k = \dim_{\mathbb{F}_p} \mathrm{H}^1(H, \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K))[p] + m(\mathfrak{X}_S(K)).$$

En vertu du lemme de Krull-Schmidt, tout $\mathbb{Z}_p[G]$-module A de type fini, où G est un p-groupe, se décompose de façon unique, à l'ordre et l'isomorphisme près des facteurs, en somme directe de sous-modules indécomposables. Il existe donc un entier $m(A)$ maximal tel que A admette un facteur direct isomorphe à $\mathbb{Z}_p[G]^{m(A)}$.

L'invariant $m(A)$ est donné par le lemme algébrique suivant (*cf.* par exemple [**JW**]).

Lemme 3.6. *Soit G un p-groupe et A un $\mathbb{Z}_p[G]$-module compact noetherien. Alors*

$$m(A) = \dim_{\mathbb{F}_p}(N_G(\mathrm{fr}_{\mathbb{Z}_p} A/p\,\mathrm{fr}_{\mathbb{Z}_p} A)),$$

où N_G désigne la norme pour G.

Preuve du Théorème 3.5: i) Montrons tout d'abord la seconde inégalité.

Notons pour cette démonstration $\mathcal{Y} = \mathcal{Y}_S(K/k)$, $\mathfrak{X} = \mathfrak{X}_S(K)$, $\mathrm{fr} = \mathrm{fr}_{\mathbb{Z}_p}$, $\mathrm{tor} = \mathrm{tor}_{\mathbb{Z}_p}$.

D'aprés 3.4, ρ_k est majoré par

$$m(\mathcal{Y}) = \dim_{\mathbb{F}_p}(N_H(\mathrm{fr}\,\mathcal{Y}/p\,\mathrm{fr}\,\mathcal{Y})).$$

Un calcul de $m(\mathcal{Y})$ grâce à des méthodes cohomologiques (inspiré de [**N5**]) va alors nous permettre de démontrer le résultat.

La définition des groupes de cohomologie modifiés pour un groupe fini, nous donne:

$$\dim_{\mathbb{F}_p} N_H(\mathrm{fr}\,\mathcal{Y}/p\,\mathrm{fr}\,\mathcal{Y}) \\ = \dim_{\mathbb{F}_p} \mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y}/p\,\mathrm{fr}\,\mathcal{Y}) - \dim_{\mathbb{F}_p} \hat{\mathrm{H}}^0(H, \mathrm{fr}\,\mathcal{Y}/p\,\mathrm{fr}\,\mathcal{Y}).$$

Considérons la suite exacte

$$\{0\} \longrightarrow \mathrm{fr}\,\mathcal{Y} \xrightarrow{p} \mathrm{fr}\,\mathcal{Y} \longrightarrow \mathrm{fr}\,\mathcal{Y}/p\,\mathrm{fr}\,\mathcal{Y} \longrightarrow \{0\}.$$

En écrivant les suites exactes longue de cohomologie et de cohomologie modifiée, on obtient les suites exactes:

$$\{0\} \longrightarrow \hat{\mathrm{H}}^0(H, \mathrm{fr}\,\mathcal{Y})/p\hat{\mathrm{H}}^0(H, \mathrm{fr}\,\mathcal{Y}) \longrightarrow \hat{\mathrm{H}}^0(H, \mathrm{fr}\,\mathcal{Y}/p\,\mathrm{fr}\,\mathcal{Y}) \\ \longrightarrow \mathrm{H}^1(H, \mathrm{fr}\,\mathcal{Y})[p] \longrightarrow \{0\}$$

et

$$\{0\} \longrightarrow \mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y})/p\mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y}) \longrightarrow \mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y}/p\,\mathrm{fr}\,\mathcal{Y}) \\ \longrightarrow \mathrm{H}^1(H, \mathrm{fr}\,\mathcal{Y})[p] \longrightarrow \{0\}.$$

Un simple calcul de dimensions nous donne alors l'expression suivante de $m(\mathcal{Y})$:

$$m(\mathcal{Y}) = \dim_{\mathbb{F}_p} \mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y})/p\mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y}) \\ - \dim_{\mathbb{F}_p} \hat{\mathrm{H}}^0(H, \mathrm{fr}\,\mathcal{Y})/p\hat{\mathrm{H}}^0(H, \mathrm{fr}\,\mathcal{Y}).$$

Donc, par trivialité cohomologique de $\mathcal{Y}$, on a

$$m(\mathcal{Y}) = \dim_{\mathbb{F}_p} \mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y})/p\mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y}) \\ - \dim_{\mathbb{F}_p} \mathrm{H}^1(H, \mathrm{Tor}\,\mathfrak{X})/p\mathrm{H}^1(H, \mathrm{Tor}\,\mathfrak{X}).$$

De plus $\mathrm{H}^1(H, \mathrm{Tor}\,\mathfrak{X})$ est fini, d'où

$$m(\mathcal{Y}) = \dim_{\mathbb{F}_p} \mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y})/p\mathrm{H}^0(H, \mathrm{fr}\,\mathcal{Y}) - \dim_{\mathbb{F}_p} \mathrm{H}^1(H, \mathrm{Tor}\,\mathfrak{X})[p].$$

Considérons la suite exacte

$$\{0\} \longrightarrow \mathrm{Tor}\,\mathfrak{X} \longrightarrow \mathcal{Y} \longrightarrow \mathrm{fr}\,\mathcal{Y} \longrightarrow 0.$$

La suite exacte de cohomologie par rapport à H nous donne, par trivialité cohomologique de $\mathcal{Y}$, la suite exacte de $\mathbb{Z}_p[[H]]$-modules

$$\{0\} \longrightarrow (\mathrm{Tor}\,\mathfrak{X})^H \longrightarrow \mathcal{Y}^H \longrightarrow (\mathrm{fr}\,\mathcal{Y})^H \longrightarrow \mathrm{H}^1(H, \mathrm{Tor}\,\mathfrak{X}) \longrightarrow \{0\}.$$

Or, sous Leopoldt, $(\mathrm{Tor}\,\mathfrak{X})^H = \mathrm{Tor}\,\mathfrak{X}_S(k)$ et il est facile de voir que $\mathcal{Y}^H = \mathfrak{X}_S(k)$.

On a alors la suite exacte:

$$\{0\} \longrightarrow \operatorname{fr}\mathfrak{X}_S(k) \longrightarrow (\operatorname{fr}\mathcal{Y})^H \longrightarrow \mathrm{H}^1(H, \operatorname{Tor}\mathfrak{X}) \to \{0\}.$$

Or $\operatorname{Tor}\mathfrak{X}$ est fini, donc $\operatorname{rang}_{\mathbb{Z}_p}(\operatorname{fr}\mathcal{Y})^H = \operatorname{rang}_{\mathbb{Z}_p} \operatorname{fr}\mathfrak{X}_S(k)$ $(= 1 + r_2)$.

Donc

$$\dim_{\mathbb{F}_p} \mathrm{H}^0(H, \operatorname{fr}\mathcal{Y})/p\mathrm{H}^0(H, \operatorname{fr}\mathcal{Y}) = \dim_{\mathbb{F}_p} \operatorname{fr}\mathfrak{X}_S(k)/p \operatorname{fr}\mathfrak{X}_S(k).$$

On obtient donc, puisque $\dim_{\mathbb{F}_p} \operatorname{fr}\mathfrak{X}_S(k)/p \operatorname{fr}\mathfrak{X}_S(k) = r_2 + 1$ sous Leopoldt,

$$m(\mathcal{Y}) = r_2 + 1 - \dim_{\mathbb{F}_p} \mathrm{H}^1(H, \operatorname{Tor}\mathfrak{X})[p].$$

D'où le résultat.

La première inégalité se déduit sans problème de ce qui précède, la suite exacte (2) et du résultat 3.4.

ii) Provient directement de ce qui précède, la suite exacte (3) et du résultat 3.4. □

Corollaire 3.7. *Soit K/k une extension finie de corps de nombres algébriques de groupe de Galois H telle que $K \subset L_{\rho_k}$. On suppose que K vérifie la conjecture de Leopoldt en p. Si $\rho_k = r_2(k) + 1$, alors*

$$\mathrm{H}^1(H, \operatorname{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K)) = 0.$$

Si de plus $d(H) = \rho_k$, alors $m(\mathfrak{X}_S(K)) = 0$.

Preuve: Immédiate.

Remarque 3.8. Grâce au corollaire précédent, en dévissant H (qui est résoluble), on se ramène au cas où H est cyclique. Le quotient de Herbrand permet alors de conclure à la trivialité cohomologique de $\operatorname{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(K)$. On retrouve ainsi le résultat 2.3.

Le Théorème 3.5ii) admet des conséquences intéressantes si l'on utilise le calcul ci-dessus pour trouver $m(\mathfrak{X}_S(K))$. En effet, on obtient l'expression:

Lemme 3.9. *Soit K une extension finie de corps de nombres algébriques de groupe de Galois H. On suppose que K vérifie la conjecture de Leopoldt en p. Alors*

$$m(\mathfrak{X}_S(K)) = r_2 + 1 - \dim_{F_p} \hat{\mathrm{H}}^0(H, \operatorname{fr}_{\mathbb{Z}_p} \mathfrak{X}_S(K))/p\hat{\mathrm{H}}^0(H, \operatorname{fr}_{\mathbb{Z}_p} \mathfrak{X}_S(K)).$$

Preuve:

$$\begin{aligned}\dim_{\mathbb{F}_p} N_H(\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)/p\,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)) &\\ = \dim_{\mathbb{F}_p}\mathrm{H}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)/p\,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)) &\\ -\dim_{\mathbb{F}_p}\hat{\mathrm{H}}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)/p\,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)).&\end{aligned}$$

Considérons la suite exacte

$$\{0\}\longrightarrow \mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)\xrightarrow{p}\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)\longrightarrow \mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)/p\,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)\longrightarrow\{0\}.$$

En écrivant les suites exactes longue de cohomologie et de cohomologie modifiée, on obtient comme précédemment l'expression suivante de $m(\mathfrak{X}_S(K))$:

$$\begin{aligned}m(\mathfrak{X}_S(K)) = \dim_{\mathbb{F}_p}\mathrm{H}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K))/p\mathrm{H}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)) &\\ -\dim_{\mathbb{F}_p}\hat{\mathrm{H}}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K))/p\hat{\mathrm{H}}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)).&\end{aligned}$$

Or, sous la conjecture de Leopoldt (*cf.* [**N5**, p. 748]),

$$\dim_{\mathbb{F}_p}\mathrm{H}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K))/p\mathrm{H}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)) = r_2+1.$$ □

Corollaire 3.10. *Soit K/k une extension finie de corps de nombres algébriques de groupe de Galois H telle que $K\subset L_{\rho_k}$. On suppose que K vérifie la conjecture de Leopoldt en p. Alors*

$$\begin{aligned}r_2+1 &\geq \rho_k+\dim_{\mathbb{F}_p}\mathrm{H}^1(H,\mathrm{Tor}_{\mathbb{Z}_p}\mathfrak{X}_S(K))[p]\\ &\geq \dim_{F_p}\hat{\mathrm{H}}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K))/p\hat{\mathrm{H}}^0(H,\mathrm{fr}_{\mathbb{Z}_p}\mathfrak{X}_S(K)).\end{aligned}$$

Preuve: Le résultat est une conséquence immédiate du lemme précédent et du Théorème 3.5. □

Lien avec la capitulation des idéaux. Soit k_∞/k, une $\mathbb{Z}_p$-extension de groupe de Galois Γ. Les résultats généraux de structure des Λ-modules montrent l'existence d'une suite exacte:

$$\{0\}\longrightarrow\mathrm{fr}_\Lambda\mathfrak{X}(k_\infty)\longrightarrow\Lambda^{r_2}\longrightarrow E\longrightarrow\{0\} \tag{3}$$

où E est un Λ-module fini.

On sait (*cf.* [**I**]) que, dans le cas où k_∞ est la $\mathbb{Z}_p$-extension cyclotomique de k, E est isomorphe au dual de Kummer de

$$\varprojlim_n(\mathrm{Ker}(A_n\longrightarrow A))$$

où A_n désigne la p-partie du groupe des S-classes de k_n et $A:=\varinjlim_n A_n$ pour $\cup k_n = k_\infty$.

Nous allons étendre la définition de ρ_k et définir $\rho_k(k_\infty) := \max_{d\in\mathbb{N}}\{\exists\ L_d \supset k_\infty$ avec $\mathrm{Gal}(L_d/k) \cong F_d\}$.

Corollaire 3.11. (i) *Avec les notations ci-dessus, en supposant que k_∞ vérifie la conjecture faible de Leopoldt et k_n vérifie la conjecture de Leopoldt, on a*

$$r_2(k) + 1 - \rho_k(k_\infty) \geq \dim_{\mathbb{F}_p} \mathrm{H}^1(\mathrm{Gal}(k_n/k), E^{\Gamma_n})[p].$$

(ii) *Si de plus, un suppose que n est assez grand pour que $E^{\Gamma_n} = E$, alors*

$$r_2(k) + 1 - \rho_k(k_\infty) \geq \frac{\dim_{\mathbb{F}_p} E[p]}{p^n}.$$

(iii) *Si l'on suppose la conjecture de Leopoldt vérifiée pour tout k_n, alors*

$$r_2(k) + 1 - \rho_k(k_\infty) \geq \dim_{\mathbb{F}_p} E_\Gamma[p].$$

Remarque 3.12. Le résultat précédent peut être rapproché de celui sur la capitulation des idéaux apparaissant dans [**LN**]. Il donne une condition suffisante pour que $r_2(k) + 1 > \rho_k(k_\infty)$.

Preuve du Corollaire 3.11: (i) Grâce au Théorème 3.5, on a,

$$1 + r_2(k) - \rho_k(k_\infty) \leq \dim_{\mathbb{F}_p} \mathrm{H}^1(\mathrm{Gal}(k_n/k), \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(k_n))[p].$$

On va décrire la cohomologie de la torsion en s'inspirant de [**N5**].

Par le lemme du serpent appliqué à la suite exacte 3 et à la suite exacte

$$\{0\} \longrightarrow \mathrm{Tor}_\Lambda \mathfrak{X}(k_\infty) \longrightarrow \mathfrak{X}(k_\infty) \longrightarrow \mathrm{fr}_\Lambda \mathfrak{X}(k_\infty) \longrightarrow \{0\},$$

on obtient les deux suites exactes:

$$\{0\} \longrightarrow (\mathrm{Tor}_\Lambda \mathfrak{X}(k_\infty))_{\Gamma_n} \longrightarrow (\mathfrak{X}(k_\infty))_{\Gamma_n} \longrightarrow (\mathrm{fr}_\Lambda \mathfrak{X}(k_\infty))_{\Gamma_n} \longrightarrow \{0\}$$

et

$$\{0\} \longrightarrow E^{\Gamma_n} \longrightarrow (\mathrm{fr}_\Lambda \mathfrak{X}(k_\infty))_{\Gamma_n} \longrightarrow (\Lambda^{r_2})_{\Gamma_n} \longrightarrow E_{\Gamma_n} \longrightarrow \{0\}.$$

Des considérations de $\mathbb{Z}_p$-rangs, en se rappelant que k_n vérifie Leopoldt donnent immédiatement la suite exacte:

$$\{0\} \longrightarrow (\mathrm{Tor}_\Lambda \mathfrak{X}(k_\infty))_{\Gamma_n} \longrightarrow (\mathrm{Tor}_{\mathbb{Z}_p}(\mathfrak{X}(k_\infty))_{\Gamma_n}) \longrightarrow E^{\Gamma_n} \longrightarrow \{0\}.$$

De plus, comme $\Gamma_n \cong \mathfrak{X}(k_n)/(\mathfrak{X}(k_\infty))_{\Gamma_n}$, on a $\mathrm{Tor}_{\mathbb{Z}_p}((\mathfrak{X}(k_\infty))_{\Gamma_n}) = \mathrm{Tor}_{\mathbb{Z}_p}(\mathfrak{X}(k_n))$, donc

$$\{0\} \longrightarrow (\mathrm{Tor}_\Lambda \mathfrak{X}(k_\infty))_{\Gamma_n} \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p}(\mathfrak{X}(k_n)) \longrightarrow E^{\Gamma_n} \longrightarrow \{0\}.$$

Mais $(\mathrm{Tor}_\Lambda \mathfrak{X}(k_\infty))_{\Gamma_n}$ est un $\mathrm{Gal}(k_n/k)$-module cohomologiquement trivial, donc

$$\mathrm{H}^1(\mathrm{Gal}(k_n/k), \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(k_n)) \cong \mathrm{H}^1(\mathrm{Gal}(k_n/k), E^{\Gamma_n}).$$

(ii) D'aprés (i), on a $r_2(k_n)+1-\rho_{k_n}(k_\infty) \geq \dim_{\mathbb{F}_p} \mathrm{H}^1(\mathrm{Gal}(k_m/k_n), E^{\Gamma_m})[p]$, pour $m > n$, d'où

$$p^n(r_2(k_n) + 1 - \rho_{k_n}(k_\infty)) \geq \dim_{\mathbb{F}_p} \mathrm{Hom}(\mathrm{Gal}(k_m/k_n), E)[p].$$

On a donc, pour $n < m$ suffisamment grand, l'isomorphisme

$$\mathrm{H}^1(\mathrm{Gal}(k_m/k_n), \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(k_n)) \cong E.$$

D'où le résultat.

(iii) est clair en passant à la limite. □

4. Expression locale-globale de $(1 + r_2) - \rho_k$

Dans cette section, on se place dans le cas particulier où k contient μ_p.

Rappelons la suite exacte suivante (*cf.* e.g. [**N3**]), pour k vérifiant la conjecture de Leopoldt en p:

$$\{0\} \longrightarrow \mu_{p^\infty}(k) \xrightarrow{\text{diag}} \bigoplus_{v \in S_p(k)} \mu_{p^\infty}(k_v) \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}(k)$$
$$\xrightarrow{\beta} \mathrm{Ker}^1_S(k, \mu_{p^\infty}) \longrightarrow \{0\},$$

où $\mathrm{Ker}^1_S(k, \bullet) := \mathrm{Ker}(\mathrm{H}^1(\mathcal{G}_S(k), \bullet) \to \oplus_{v \in S} \mathrm{H}^1(\mathcal{G}_v, \bullet))$ avec $\mathcal{G}_S$ le groupe de Galois sur k de l'extension algébrique S-ramifiée maximale de k (G_S est donc le pro-p-quotient maximal de $\mathcal{G}_S$) et pour toute place $v \in S$, $\mathcal{G}_v$ le groupe de Galois absolu de k_v.

On note $W_k := \mathrm{Ker}\,\beta \cong \mathrm{Coker}(\mathrm{diag})$. Cette définition étant valable pour toute extension finie de k, on définit W_K pour une extension K/k infinie par limite inductive. On a alors les suites exactes de $\mathrm{Gal}(K/k)$-modules:

$$\{0\} \longrightarrow \mu_{p^\infty}(K) \xrightarrow{\text{diag}} \bigoplus_{v \in S_p(k)} \mathrm{Ind}_{\mathrm{Gal}(K_v/k)}^{\mathrm{Gal}(K/k)} \mu_{p^\infty}(K_v) \longrightarrow W_K \longrightarrow \{0\}$$

et

$$(4) \qquad \{0\} \longrightarrow W_K \longrightarrow \varinjlim_n \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}(k_n) \longrightarrow \mathrm{Ker}^1_S(K, \mu_{p^\infty}) \longrightarrow \{0\},$$

pour toute extension K/k, où $\varinjlim_n k_n = K$.

Remarque 4.1. En vertu de [**N3**], on a $W_{k_S} = I_2(G_S)$, le module dualisant de G_S.

Pour une place v de k, on note F_v, le groupe de décomposition de F_{ρ_k} pour une place choisie de L_{ρ_k} au-dessus de v. On a alors le

Théorème 4.2. *Soit k un corps de nombres algébriques contenant μ_p. Soit L_{ρ_k}/k, F_{ρ_k}-extension cyclotomique ($\mu_{p^\infty} \subset L_{\rho_k}$) telle que toutes les sous-extensions finies de L_{ρ_k}/k vérifient la conjecture de Leopoldt en p, alors*

$$r_2(k) + 1 - \rho_k = \sum_{v \in S_p(k)} \left(\frac{n_v}{2} + 1 - \rho_v\right) + \dim_{\mathbb{F}_p} \mathrm{H}^1(F_{\rho_k}, W_{L_{\rho_k}})[p],$$

où ρ_v est le rang de F_v, qui est un pro-p-groupe libre.

Preuve: On a évidemment

$$r_2(k) + 1 - \rho_k = \sum_{v \in S_p(k)} \frac{n_v}{2} + 1 - \rho_k.$$

Calculons maintenant $1-\rho_k$ en posant $\rho := \rho_k$, $L := L_{\rho_k}$ et $F := F_{\rho_k}$. Pour cela considérons la suite exacte:

$$\{0\} \longrightarrow \mu_{p^\infty}(L) \longrightarrow \bigoplus_{v \in S_p(k)} \mathrm{Ind}_{(F)_v}^{F_\rho} \mu_{p^\infty}(L_v) \longrightarrow W_L \longrightarrow \{0\}.$$

La suite exacte longue de cohomologie par rapport à F nous donne alors:

$$\begin{aligned}\{0\} \longrightarrow \mu_{p^\infty}(k) \longrightarrow \bigoplus_{v \in S_p} \mu_{p^\infty}(k_v) \longrightarrow W_L^F \longrightarrow \mathrm{H}^1(F, \mu_{p^\infty}(L))\\ \longrightarrow \bigoplus_{v \in S_p} \mathrm{H}^1(F_v, \mu_{p^\infty}(L_v)) \longrightarrow \mathrm{H}^1(F, W_L) \longrightarrow \{0\}.\end{aligned}$$

On sait (*cf.* [**W1**]) que $(\varinjlim_n \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}(k_n))^F = \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(k)$ où $\varinjlim_n k_n = L_{r_2+1}$, donc la cohomologie de la suite exacte (4) montre que W_L^F est fini, en tant que sous-module de $\mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_S(k)$. Un simple calcul de corang nous donne alors:

$$\rho - 1 = \sum_{v \in S_p} (\rho_v - 1) - \dim_{\mathbb{F}_p} \mathrm{H}^1(F, W_L)[p].$$

D'où le résultat. $\square$

Corollaire 4.3. *Avec les hypothèses sur k du théorème, les assertions suivantes sont équivalentes:*

(i) $\rho_k = r_2(k) + 1$.
(ii) $\rho_v = \frac{n_v}{2} + 1$ *pour tout* $v \in S_p$ *et* $\mathrm{H}^1(F_{\rho_k}, W_{L_{\rho_k}}) = 0$.

Preuve: En effet, on sait que $\rho_v \leq \frac{n_v}{2} + 1$. □

Lien avec le module dualisant. L'expression précédente fait apparaître un module $W_{L_{\rho_k}}$ qui est lié au module dualisant de $G_S(k)$ par la suite exacte ($L = L_{\rho_k}$)

$$\{0\} \longrightarrow W_L \longrightarrow I_2(G_S(k))^{G_S(L)} \longrightarrow \ker^1_S(L, \mu_{p^\infty}) \longrightarrow \{0\},$$

où $\ker^1_S(L, \mu_{p^\infty})$ est le noyau du morphisme naturel:

$$\mathrm{H}^1(\mathrm{Gal}(k_S/L), \mu_{p^\infty}) \longrightarrow \bigoplus_{v \in S(L)} \mathrm{H}^1(\mathrm{Gal}(k_v(p)/L_v), \mu_{p^\infty})$$

avec $k_v(p)$ la pro-p-extension absolue de k_v, le complété en v de k.

Ce dernier module admet une interprétation galoisienne, puisque, dans notre cas, il est isomorphe au dual de Kummer du conoyau de

$$\bigoplus_{v \in S(L)} \mathfrak{X}(L_v) \xrightarrow{\text{nat.}} \mathfrak{X}(L)$$

où $\mathfrak{X}(L_v)$ est le groupe de Galois de la pro-p-extension abélienne maximale du complété L_v. On a donc les isomorphismes

$$\begin{aligned} \ker^1_S(L, \mu_{p^\infty}) &\cong \{x \in L^*/x \in L_v^* \quad \forall\, v \in S,\, x \in U_v^* \quad \forall\, v \notin S\} \\ &\cong \mathrm{Hom}_{F_{\rho_k}}(X(L_{\rho_k}), \mu_{p^\infty}) \end{aligned}$$

où U_v désigne les unités de L_v, $X(L_{\rho_k}) := \varprojlim_n X(k_n)$, avec $X(k_n)$ le groupe de Galois de la p-extension maximale non-ramifiée et p-décomposée de k_n, et $\cup_{n \in \mathbb{N}} k_n = L_{\rho_k}$.

Ce lien nous permet d'obtenir le théorème suivant:

Théorème 4.4. *Soit k un corps de nombres algébriques contenant μ_p. Soit L_{ρ_k}/k, F_{ρ_k}-extension cyclotomique ($\mu_{p^\infty} \subset L_{\rho_k}$) telle que toutes les sous-extensions finies de L_{ρ_k}/k vérifient la conjecture de Leopoldt en p, alors*

$$m(\mathfrak{X}_{S_p}(K)) = \sum_{v \in S_p(k)} \left(\frac{n_v}{2} + 1 - \rho_v\right) - \dim_{\mathbb{F}_p} \mathrm{H}^1(F_{\rho_k}, \ker^1_{S_p}(L_{\rho_k}, \mu_{p^\infty}))[p],$$

où K est tel que $d(\mathrm{Gal}(K/k)) = \rho_k$.

Preuve: 1) Montrons tout d'abord que

$$r_2(k)+1-\rho_k=\sum_{v\in S_p(k)}\Big(\frac{n_v}{2}+1-\rho_v\Big)+\mathrm{rang}_{\mathbb{Z}_p}(\mathrm{H}^1(F_{\rho_k},I_2(G_{S_p}(k))^{G_{S_p}(L)}))^* \\ -\mathrm{rang}_{\mathbb{Z}_p}(\mathrm{H}^1(F_{\rho_k},\ker^1_{S_p}(L,\mu_{p^\infty})))^*.$$

La suite exacte

$$\{0\}\longrightarrow W_L\longrightarrow I_2(G_S(k))^{G_S(L)}\longrightarrow \ker^1_S(L,\mu_{p^\infty})\longrightarrow\{0\}$$

nous donne la suite exacte longue de cohomologie

$$\ker^1_S(L,\mu_{p^\infty})^{F_{\rho_k}}\longrightarrow \mathrm{H}^1(F_{\rho_k},W_L)\longrightarrow \mathrm{H}^1(F_{\rho_k},I_2(G_S(k))^{G_S(L)}) \\ \twoheadrightarrow \mathrm{H}^1(F_{\rho_k},\ker^1_S(L,\mu_{p^\infty}))$$

où $L=L_{\rho_k}$.

Pour avoir le résultat, il suffit donc de montrer que $\ker^1_S(L_{\rho_k},\mu_{p^\infty})^{F_{\rho_k}}$ est fini.

Or le lemme du serpent nous donne le diagramme commutatif:

$$\begin{array}{ccccccccc}
 & & \{0\} & & \{0\} & & \{0\} & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
\{0\} & \to & \mathrm{Ker}^1_{S_p}(L,\mu_{p^\infty})^F & \to & \mathrm{H}^1(G_{S_p}(L),\mu_{p^\infty})^F & \to & \bigoplus_{v\in S_p(k)}\mathrm{H}^1(\mathrm{Gal}((k_{S_p})_v/L_v),\mu_{p^\infty})^{F_v} & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
\{0\} & \to & \mathrm{Ker}^1_{S_p}(k,\mu_{p^\infty}) & \to & \mathrm{H}^1(G_{S_p}(k),\mu_{p^\infty}) & \to & \bigoplus_{v\in S_p(k)}\mathrm{H}^1(\mathrm{Gal}((k_{S_p})_v/k_v),\mu_{p^\infty}) & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
\{0\} & \to & W_L^F/W_k & \to & \mathrm{H}^1(F,\mu_{p^\infty}) & \to & \bigoplus_{v\in S_p(k)}\mathrm{H}^1(F_v,\mu_{p^\infty}) & \to & \{0\} \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \{0\} & & \{0\} & & \{0\}, & &
\end{array}$$

où $F:=F_{r_2+1}$.

D'où le résultat.

2) Montrons le théorème.

$W_{L_{\rho_k}}$ est divisible. On a donc la suite exacte

$$\{0\}\longrightarrow W_{L_{\rho_k}}[p]\longrightarrow W_{L_{\rho_k}}\xrightarrow{\times p} W_{L_{\rho_k}}\longrightarrow\{0\},$$

ce qui implique par cohomologie

$$\mathrm{H}^1(F_{\rho_k}, W_{L_{\rho_k}}) \twoheadrightarrow \mathrm{H}^1(F_{\rho_k}, W_{L_{\rho_k}}).$$

Donc $\mathrm{H}^1(F_{\rho_k}, W_{L_{\rho_k}})$ est divisible. La comparaison du théorème précédent avec le Théorème 3.5 donne immédiatement le résultat. □

Références

[Br] A. BRUMER, Pseudocompact algebras, profinite groups and class formations, *J. Algebra* **4** (1966), 442–470.

[GJ] G. GRAS ET J.-F. JAULENT, Sur les corps de nombres réguliers, *Math. Z.* **202(3)** (1989), 343–365.

[GW] K. W. GRUENBERG ET A. WEISS, Galois invariants for units, *Proc. London Math. Soc. (3)* **70(2)** (1995), 264–284.

[Ha] K. HABERLAND, *"Galois cohomology of algebraic number fields"*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.

[I] K. IWASAWA, On $\mathbf{Z}_l$-extensions of algebraic number fields, *Ann. of Math. (2)* **98** (1973), 246–326.

[J] U. JANNSEN, Iwasawa modules up to isomorphism, in: *"Algebraic number theory"*, Adv. Stud. Pure Math. **17**, Academic Press, Boston, MA, 1989, pp. 171–207.

[JW] U. JANNSEN ET K. WINGBERG, Die p-vervollständigung der multiplikativen gruppe einer p-erweiterung eines irregulären p-adischen zahlkörpers, *J. Reine angew. Math.* **307/308** (1979), 399–410.

[LN] A. LANNUZEL ET T. NGUYEN QUANG DO, Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres, *Manuscripta Math.* **102(2)** (2000), 187–209.

[MN] A. MOVAHHEDI ET T. NGUYEN QUANG DO, Sur l'arithmétique des corps de nombres p-rationnels, in: *"Séminaire de Théorie des Nombres"* (Paris 1987–88), Progr. Math. **81**, Birkhäuser Boston, Boston, MA, 1990, pp. 155–200.

[NSW] J. NEUKIRCH, A. SCHMIDT ET K. WINGBERG, *"Cohomology of number fields"*, Grundlehren der Mathematischen Wissenschaften **323**, Springer-Verlag, Berlin, 2000.

[N1] T. NGUYEN QUANG DO, Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa, *Compositio Math.* **46(1)** (1982), 85–119.

[N2] T. NGUYEN QUANG DO, Formations de classes et modules d'Iwasawa, in: *"Number theory"* (Noordwijkerhout, 1983), Lecture Notes in Math. **1068**, Springer, Berlin, 1984, pp. 167–185.

[N3] T. Nguyen Quang Do, Sur la $\mathbf{Z}_p$-torsion de certains modules galoisiens, *Ann. Inst. Fourier (Grenoble)* **36(2)** (1986), 27–46.

[N4] T. Nguyen Quang Do, Sur la structure Galoisienne des corps locaux et la théorie d'Iwasawa. II, *J. Reine angew. Math.* **333** (1982), 133–143.

[N5] T. Nguyen Quang Do, Sur la cohomologie de certains modules galoisiens p-ramifiés, in: *"Théorie des nombres"* (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 740–754.

[W1] K. Wingberg, On Galois groups of p-closed algebraic number fields with restricted ramification, *J. Reine angew. Math.* **400** (1989), 185–202.

[W2] K. Wingberg, On Galois groups of p-closed algebraic number fields with restricted ramification. II, *J. Reine angew. Math.* **416** (1991), 187–194.

[W3] K. Wingberg, Galois groups of local and global type, *J. Reine angew. Math.* **517** (1999), 223–239.

[Y1] M. Yamagishi, A note on free pro-p-extensions of algebraic number fields, *J. Théor. Nombres Bordeaux* **5(1)** (1993), 165–178.

[Y2] M. Yamagishi, A note on free pro-p-extensions of algebraic number fields. II, *Manuscripta Math.* **91(2)** (1996), 231–233.

Laboratoire de Mathématiques (CNRS)
Université de Franche-Comté (Besançon)
25030 Besançon
France
E-mail address: `lannuz@math.univ-fcomte.fr`

Primera versió rebuda el 13 de juny de 2001,
darrera versió rebuda el 5 de desembre de 2001.