Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé

Thong NGUYEN QUANG DO

Institut des Hautes Études Scientifiques
35, route de Chartres
91440 – Bures-sur-Yvette (France)

Juillet 2005

IHES/M/05/20

Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé

Nguyen Quang Do Thong

Université de Franche-Comté, CNRS UMR 6623, 16 route de Gray, 25030 Besançon cedex, France
et
Institut des Hautes Études Scientifiques, 35 route de Chartres, 91440 Bures-sur-Yvette, France

Abstract

Let p be an odd prime. For any CM number field K containing a primitive p^{th}-root of unity, class field theory and Kummer theory put together yield the well known reflection inequality $\lambda^+ \leq \lambda^-$ between the “plus” and “minus” parts of the λ-invariant of K. Greenberg's classical conjecture predicts the vanishing of λ^+. We propose a weak form of this conjecture : $\lambda^+ = \lambda^-$ if and only if $\lambda^+ = \lambda^- = 0$, and we prove it when K^+ is abelian, p is totally split in K^+, and certain (mild) conditions on the cohomology of circular units are satisfied.

Key words: λ-invariant, circular units, universal norms

Dédié à Ralph Greenberg pour son 60$^{\text{ème}}$ anniversaire

1 Introduction

Pour tout corps de nombres totalement réel F et tout nombre premier impair p, la conjecture de Greenberg (notée (GC)) prédit que le module d'Iwasawa non ramifié $X_\infty = X_\infty(F)$ attaché à la $\mathbb{Z}_p$-extension cyclotomique F_∞ de F est fini, autrement dit que les invariants $\mu(F)$ et $\lambda(F)$ associés sont nuls (voir [6]). La nullité de $\mu(F)$ dans le cas abélien est un théorème de Ferrero-Washington. Mais la nullité de $\lambda(F)$, bien qu'elle ait été vérifiée dans certains cas particuliers et par de nombreux exemples numériques (voir [7]), n'est confirmée à l'heure actuelle par aucun résultat théorique général. Dans cet article, on se concentrera sur la nullité conjecturale de l'invariant $\lambda(F)$, en direction de laquelle on démontrera un résultat assez général qui peut être considéré comme une version affaiblie de (GC). Plus précisément :

Soit $\mathcal{X}_\infty = \mathcal{X}_\infty(F)$ le module d'Iwasawa p-ramifié (c'est-à-dire non ramifié en dehors des p-places) attaché à F_∞. D'après la conjecture faible de Leopoldt – qui est vérifiée par la $\mathbb{Z}_p$-extension cyclotomique – le module $\mathcal{X}_\infty$ est de Λ-torsion, et l'on notera $\tilde{\mu}(F)$ et $\tilde{\lambda}(F)$ ses invariants d'Iwasawa. La surjection canonique $\mathcal{X}_\infty \twoheadrightarrow X_\infty$ entraîne les inégalités $\tilde{\mu}(F) \geq \mu(F)$ et $\tilde{\lambda}(F) \geq \lambda(F)$. Notons que si F est le sous-corps totalement réel maximal d'un corps K qui est CM et qui contient une racine primitive $p^{\text{ième}}$ de l'unité, la décomposition habituelle suivant les valeurs propres ± 1 de la conjugaison complexe donne les relations : $\mu(K) = \mu(K)^- + \mu(F)$, $\lambda(K) = \lambda(K)^- + \lambda(F)$, alors que la théorie de Kummer et la théorie de l'adjoint d'Iwasawa donnent : $\tilde{\mu}(K^+) = \mu(K)^-$ et $\tilde{\lambda}(K^+) = \lambda(K)^-$, de sorte que les inégalités précédentes ne sont autres que les *inégalités du miroir* ("Spiegelung") bien connues $\mu(K)^- \geq \mu(F)$ et $\lambda(K)^- \geq \lambda(F)$. Dans ce cas, si la conjecture (GC) est vraie, les inégalités du miroir sont strictes, sauf si les invariants "moins" sont triviaux. Cela justifie d'introduire la forme faible suivante de la conjecture de Greenberg (voir [3], [8]) :

(GF) $\tilde{\lambda}(F) = \lambda(F)$ et $\tilde{\mu}(F) = \mu(F)$ *si et seulement si tous ces invariants sont nuls.*

Remarques.

1) La nullité simultanée de $\tilde{\mu}(F)$ et $\tilde{\lambda}(F)$ signifie la nullité du module $\mathcal{X}_\infty$, c'est-à-dire que l'arithmétique du corps F devient "triviale" en p.
2) Soit $G_F(T) \in \Lambda := \mathbb{Z}_p[[T]]$ la série caractéristique de $\mathcal{X}_\infty$. D'après la Conjecture Principale (ou théorème de Wiles), on sait que cette série est reliée aux fonctions L_p attachées à F. On peut montrer ([3], corollaire 1.5) que si $G_F(T)$ est irréductible, alors les conjectures (GF) et (GC) sont équivalentes, et donc (GF) n'est pas si faible qu'elle en a l'air.

Dans [3], on a vérifié la conjecture (GF) dans un certain nombre de cas particuliers, mais la situation était la même que pour (GC), à savoir qu'on n'avait pas de résultat positif théorique et général. Le but du présent travail est de démontrer le

Théorème principal. *Si F est un corps abélien réel tel que p est totalement décomposé dans F et p ne divise pas le degré $[F : \mathbb{Q}]$, alors F vérifie la conjecture (GF) pour p.*

En vertu de la remarque 2), cela donne un résultat assez général en direction de la conjecture de Greenberg.

2 Une traduction de la conjecture (GF)

Il s'agit de traduire la conjecture (GF) en termes (autant que possible) non asymptotiques. Les calculs ont été faits essentiellement dans [3], mais nous les reprenons rapidement pour la commodité du lecteur. Fixons d'abord les notations : F désigne un corps de nombres totalement réel, $F_\infty = \bigcup_{n\geq 0} F_n$ sa $\mathbb{Z}_p$-extension cyclotomique, $\Gamma = \mathrm{Gal}(F_\infty/F)$, A_n le p-groupe de classes de F_n, $X_\infty = \varprojlim A_n$. Par le corps de classes, X_∞ est isomorphe au groupe de Galois de la pro-p-extension abélienne non ramifiée maximale de F_∞. Introduisons aussi $\mathcal{X}_\infty$ (resp. $\mathcal{X}_n$), le groupe de Galois de la pro-p-extension abélienne p-ramifiée maximale de F_∞ (resp. F_n). Nous écrirons souvent A_F, $\mathcal{X}_F$ etc ... au lieu de A_0, $\mathcal{X}_0$ etc ... Comme d'habitude, on notera M^Γ (resp. M_Γ) les invariants (resp. co-invariants) de M par l'action de Γ.

Pour simplifier, on supposera à partir de maintenant que tous les F_n *vérifient la conjecture de Leopoldt en* p.

2.1. Lemme. *L'égalité des invariants* λ *et* μ *de* $\mathcal{X}_\infty$ *et* X_∞ *équivaut à la conjonction des deux propriétés suivantes :*

(GF1) *Le sous-module fini maximal* X^0_∞ *de* X_∞ *est nul*

et

(GF2) *La surjection naturelle* $(\mathcal{X}_\infty)_\Gamma \twoheadrightarrow (X_\infty)_\Gamma$ *est un isomorphisme.*

Preuve. Considérons la suite exacte de Λ-modules : $0 \to I_\infty \to \mathcal{X}_\infty \to X_\infty \to 0$, où I_∞ est le sous-groupe d'inertie pour toutes les p-places de F_∞. Les invariants λ et μ de $\mathcal{X}_\infty$ et X_∞ sont égaux si et seulement si I_∞ est fini, c'est-à-dire nul puisqu'il est bien connu que $\mathcal{X}_\infty$ n'a pas de sous-module fini non nul. Or le lemme du serpent pour l'action de Γ donne une suite exacte :

$$(\mathcal{X}_\infty)^\Gamma \to (X_\infty)^\Gamma \to (I_\infty)_\Gamma \to (\mathcal{X}_\infty)_\Gamma \to (X_\infty)_\Gamma \to 0\,.$$

Par la conjecture de Leopoldt pour F, il est bien connu que $(\mathcal{X}_\infty)^\Gamma$ est nul et $(X_\infty)^\Gamma$ est fini. Par le lemme de Nakayama, il s'ensuit que I_∞ est nul si et seulement si X^0_∞ est nul et $(\mathcal{X}_\infty)_\Gamma \twoheadrightarrow (X_\infty)_\Gamma$ est un isomorphisme. □

La condition (GF2), qui se situe au niveau du corps de base F, est de type analytique p-adique : par Leopoldt, on sait que $(\mathcal{X}_\infty)_\Gamma \simeq \mathrm{tor}_{\mathbb{Z}_p}\mathcal{X}_F$, et l'ordre de ce dernier module s'exprime en termes de régulateur-discriminant (formule de Coates) ou du résidu en $s = 1$ de la fonction zêta p-adique de F (Conjecture Principale) ; pour des détails, voir e.g. [13]. Heureusement :

2.2. Lemme. (Ozaki-Taya) *Si le corps* F *est* p*-décomposé (i.e.* p *se décompose* *totalement dans F), la condition (GF2) est automatiquement vérifiée.*

Preuve. Voir e.g. [3], lemme 3.1. $\square$

La condition (GF1), quant à elle, est de type asymptotique, le sous-module fini maximal X_∞^0 étant intimement lié à la capitulation des idéaux dans F_∞, un problème compliqué qui a fait l'objet de nombreux travaux ([11], [9], etc ...). L'idée – inspirée de l'étude faite dans [6] de la conjecture de Greenberg dans le cas p-décomposé – va être d'introduire un sous-module de p-décomposition $D_\infty \subseteq X_\infty^0$. Plus précisément, pour tout $n \geq 0$, soit A'_n le p-groupe des classes de (p)-idéaux de F_n, défini par une suite exacte : $0 \to D_n \to A_n \to A'_n \to 0$, où D_n est l'image dans A_n du sous-groupe des classes de F_n engendré par les classes des idéaux au-dessus de p. Soit $0 \to D_\infty \to X_\infty \to X'_\infty \to 0$ la suite exacte de Λ-modules obtenue par passage à la limite projective sur les normes. Par Leopoldt pour tous les F_n, on sait que les D_n sont finis bornés ([6], [16], etc ...), donc que D_∞ est fini, et par conséquent $D_\infty \subseteq X_\infty^0$. Dans la suite nous aurons seulement besoin de cette inclusion, mais notons la caractérisation suivante de D_∞ dans le cas p-décomposé :

2.3. Lemme. *Si F est p-décomposé, alors $D_\infty \simeq (X_\infty^0)^\Gamma$.*

Preuve. Voir [3], lemme 3.2. $\square$

D'après 1.1 et 1.2, la conjecture (GF) dans le cas p-décomposé revient à dire que la nullité de X_∞^0 entraîne celle de X_∞. Pour démontrer cela dans le cas abélien, l'idée de départ sera de remplacer le p-groupe des classes A_n par le quotient $B_n := \bar{U}_n/\bar{C}_n$, où $\bar{U}_n$ (resp. $\bar{C}_n$) désigne le complété p-adique du groupe des unités (resp. des unités circulaires) de F_n. La descente galoisienne sur le module $B_\infty := \varinjlim B_n$ (limite inductive pour les applications naturelles induites par l'inclusion) dépend de la cohomologie des modules $\bar{U}_n$ et $\bar{C}_n$. La cohomologie de $\bar{U}_n$ peut se calculer en fonction de D_n (thm. 3.1), celle de $\bar{C}_n$ en fonction d'un certain groupe fini $t\Phi$ attaché à F (thm. 4.6). La nullité de D_∞ et de $t\Phi$ entraîne une "bonne" descente (lemme 5.3), et un calcul de Γ-quotient de Herbrand à partir de la Conjecture Principale (lemme 5.4) permet de conclure.

3 Cohomologie des unités

Si $F_\infty = \bigcup_{n \geq 0} F_n$ est la $\mathbb{Z}_p$-extension cyclotomique de F, on note U_n (resp. U'_n) le groupe des unités (resp. (p)-unités) de F_n, $U_\infty = \varinjlim U_n$, $U'_\infty = \varinjlim U'_n$, $G_n = \mathrm{Gal}(F_n/F)$, $\Gamma = \mathrm{Gal}(F_\infty/F)$, $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$, et l'on se propose de calculer les groupes de cohomologie $H^i(G_n, U_n)$ et $H^i(\Gamma, U_\infty)$, $i = 1, 2$. Il existe des résultats généraux dans ce sens, dûs principalement à Iwasawa :

– pour $i = 1, 2$, les quantités $n(s+1-i) - \mathrm{ord}_p H^i(G_n, U_n)$ sont bornées pour $n \gg 0$ ([10], p. 199). Ici, s désigne le nombre des p-places de F_∞ et ord_p la valuation p-adique normalisée par $\mathrm{ord}_p(p) = 1$

– on a un isomorphisme $H^2(\Gamma, U_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{s-1}$ et un pseudo-isomorphisme $H^1(\Gamma, U_\infty) \sim (\mathbb{Q}_p/\mathbb{Z}_p)^s$ ([10], p. 197).

Mais ces résultats ne sont pas assez précis pour notre usage, et nous nous proposons de les affiner en faisant intervenir les modules de décomposition D_n du §2. Fixons les hypothèses : F est un corps de nombres totalement réel, et nous supposons dans cette section qu'en plus :

(a) *Tous les étages F_n vérifient la conjecture de Leopoldt en p*

(b) *Toutes les p-places de F sont totalement ramifiées dans F_∞* (de sorte que la quantité s précédemment introduite est aussi le nombre des p-places de F).

On rappelle que A_n (resp. A'_n) désigne le p-groupe des classes d'idéaux (resp. des (p)-classes d'idéaux) de F_n. On notera $A_\infty = \varinjlim A_n$, $A'_\infty = \varinjlim A'_n$, $X_\infty = \varprojlim A_n$, $X'_\infty = \varprojlim A'_n$.

3.1. Théorème. *Sous les hypothèses précédentes :*

(i) Pour $i = 1, 2$, pour tout $n \geq 0$, on a

$$n(s+1-i) - \mathrm{ord}_p|H^i(G_n, U_n)| = \mathrm{ord}_p|D_n| - \mathrm{ord}_p|D_0| - \mathrm{ord}_p|\ker(A'_0 \to A'_n)|$$

(ii) $H^2(\Gamma, U_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{s-1}$ et l'on a une suite exacte de groupes abéliens

$$0 \to D_0 \oplus (\mathbb{Q}_p/\mathbb{Z}_p)^s \to H^1(\Gamma, U_\infty) \to \ker(A'_0 \to A'_\infty) \to 0\,.$$

Preuve. Soit S_n l'ensemble des p-places de F_n (de cardinal s). Soit $\bar{U}_n = U_n \otimes \mathbb{Z}_p$ (resp. $\bar{U}'_n = U'_n \otimes \mathbb{Z}_p$) le complété p-adique de U_n (resp. U'_n). La valuation p-adique induit une suite exacte $0 \to \bar{U}'_n/\bar{U}_n \to \mathbb{Z}_p[S_n] \to D_n \to 0$ qui montre, puisque D_n est fini, que $\bar{U}'_n/\bar{U}_n \simeq \mathbb{Z}_p^s$, avec action triviale de G_n (par (b)). La suite exacte tautologique $0 \to \bar{U}_n \to \bar{U}'_n \to \bar{U}'_n/\bar{U}_n \to 0$ donne alors, par cohomologie, une suite exacte :

$$0 \to \bar{U}'_0/\bar{U}_0 \xrightarrow{i_n} \bar{U}'_n/\bar{U}_n \to H^1(G_n, \bar{U}_n) \to H^1(G_n, \bar{U}'_n) \to \mathrm{Hom}(G_n, \mathbb{Z}_p^s) = 0\,. \tag{1}$$

Pour calculer $\mathrm{coker}\, i_n$, considérons le diagramme commutatif (où les flèches verticales sont induites par l'inclusion)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \bar{U}'_n/\bar{U}_n & \longrightarrow & \mathbb{Z}_p[S_n] & \longrightarrow & D_n & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle i_n} & & \uparrow{\scriptstyle j_n} & & \uparrow & & \\
0 & \longrightarrow & \bar{U}'_0/\bar{U}_0 & \longrightarrow & \mathbb{Z}_p[S_0] & \longrightarrow & D_0 & \longrightarrow & 0
\end{array}$$

Par l'hypothèse de ramification (b), $\ker j_n = 0$ et $\operatorname{coker} j_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^s$. Le lemme du serpent donne alors une suite exacte :

$$0 \to \ker(D_0 \to D_n) \to \operatorname{coker} i_n \to (\mathbb{Z}/p^n\mathbb{Z})^s \to \operatorname{coker}(D_0 \to D_n) \to 0\,. \quad (2)$$

On en déduit : $ns - \operatorname{ord}_p|H^1(G_n, \bar{U}_n)| = \operatorname{ord}_p|D_n| - \operatorname{ord}_p|D_0| - \operatorname{ord}_p H^1(G_n, \bar{U}'_n)$. Comme G_n est un p-groupe et U_n et U'_n sont sans p-torsion (car $p \neq 2$ et F est totalement réel), $H^i(G_n, \bar{U}_n) \simeq H^i(G_n, U_n)$ et $H^i(G_n, \bar{U}'_n) \simeq H^i(G_n, U'_n)$. De plus, il est bien connu que $H^1(G_n, U'_n) \simeq \ker(A'_0 \to A'_n)$ ([9], [11], ...), donc on a montré l'assertion (i) du théorème pour H^1. Pour H^2, il suffit de remarquer que le G_n-quotient de Herbrand $|H^1(G_n, U_n)|/|H^2(G_n, U_n)|$ est bien connu et vaut p^n.

Pour montrer l'assertion (ii), passons à la limite inductive sur les suites exactes (2). Pratiquement par définition, on sait que $\varinjlim D_n = 0$ et l'on obtient à l'infini une suite exacte : $0 \to D_0 \to \varinjlim \operatorname{coker} i_n \to (\mathbb{Q}_p/\mathbb{Z}_p)^s \to 0$, qui montre qu'en tant que groupe abélien, $\varinjlim \operatorname{coker} i_n \simeq D_0 \oplus (\mathbb{Q}_p/\mathbb{Z}_p)^s$, d'où la propriété cherchée pour H^1. Pour H^2, la propriété est essentiellement algébrique : en effet, $H^2(\Gamma, U_\infty)$ est p-divisible car $cd_p\Gamma = 1$; il suffit alors de calculer son co-rang, ce qui se fait facilement à partir de (i). $\square$

3.2. Corollaire. *Supposons que le sous-module fini maximal X^0_∞ est nul. Alors, pour $i = 1, 2$, $H^i(G_n, U_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{s+1-i}$ pour tout n, et $H^i(\Gamma, U_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{s+1-i}$.*

Preuve. La nullité de X^0_∞ entraîne celle de $D_\infty = \varprojlim D_n$. Comme les applications de norme $D_{n+1} \to D_n$ sont surjectives (par l'hypothèse de ramification (b)), $D_\infty = (0)$ si et seulement si $D_n = (0)$ pour tout n, i.e. $A_n \simeq A'_n$ pour tout n, d'où $X_\infty \simeq X'_\infty$, et finalement, le sous-module fini maximal $(X'_\infty)^0$ est nul. Mais on sait ([11], [9], ...) que $(X'_\infty)^0 \simeq \ker(A'_m \to A'_\infty) \simeq H^1(\Gamma_m, U'_\infty)$ pour $m \gg 0$. Comme $cd_p\Gamma = 1$, les applications de corestriction $H^1(\Gamma_{n+1}, U'_\infty) \to H^1(\Gamma_n, U'_\infty)$ sont surjectives pour tout n, et par suite la nullité de $(X'_\infty)^0$ équivaut à la nullité de tous les $H^1(\Gamma_n, U'_\infty)$.

Passons maintenant au calcul des $H^i(G_n, U_n)$:

- la nullité de $H^1(\Gamma, U'_\infty)$ entraîne, par inflation, la nullité de tous les $H^1(G_n, U'_n)$. En retournant aux suites exactes (1) et (2) de la preuve de 3.1, on en déduit immédiatement que $H^1(G_n, U_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^s$
- de la suite exacte de valuation $0 \to \bar{U}_n \to \bar{U}'_n \to \mathbb{Z}_p[S_n] \to D_n = (0)$, on déduit par cohomologie : $0 \to H^2(G_n, U_n) \to H^2(G_n, U'_n) \to H^2(G_n, \mathbb{Z}_p[S_n])$. Mais $H^2(G_n, \mathbb{Z}_p[S_n]) \simeq \hat{H}^0(G_n, \mathbb{Z}_p[S_n]) = 0$ par l'hypothèse de ramification (b). Il reste à calculer $H^2(G_n, U'_n)$. Or la nullité de $H^1(\Gamma_n, U'_\infty)$ permet d'écrire la suite exacte d'inflation-restriction $0 \to H^2(G_n, U'_n) \to H^2(\Gamma, U'_\infty) \to H^2(\Gamma_n, U'_\infty)^{G_n}$, et $H^2(\Gamma, U'_\infty) \simeq H^2(\Gamma, U_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{s-1}$ d'après ce qu'on vient de voir. Comme $H^2(G_n, U_n)$ est

d'ordre $p^{n(s-1)}$ d'après 3.1 (i), on a nécessairement l'isomorphisme $H^2(G_n, U_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{s-1}$. □

4 Cohomologie des unités circulaires

Soit maintenant F un corps *abélien* réel, vérifiant l'hypothèse (b) du §3 (l'hypothèse (a) devient automatique). Pour tout $n \geq 0$, on note $C_n = C(F_n)$ le groupe des unités circulaires de Sinnott (voir [14]) du corps F_n, et l'on se propose de calculer la G_n-cohomologie de C_n. Ce calcul a été fait dans [1] moyennant deux hypothèses restrictives :

- l'extension $F/\mathbb{Q}$ est non ramifiée en p
- le corps F vérifie une certaine condition appelée (HB) ([1], p. 34), trop technique pour être détaillée ici, mais qui est satisfaite dans un grand nombre de cas "usuels", en particulier *dans le cas semi-simple* ([1] , IV-1, p. 43).

Notre but va être de relâcher au maximum ces hypothèses restrictives, de façon à pousser les calculs le plus loin possible dans le cadre le plus général possible. La méthode, s'appuyant sur [1] et [2], consiste à introduire les sous-modules $\tilde{C}_n$ de *normes universelles d'unités circulaires*. Plus précisément, notons $\bar{U}_\infty = \varprojlim \bar{U}_n$, $\bar{U}'_\infty = \varprojlim \bar{U}'_n$, $\bar{C}_n = C_n \otimes \mathbb{Z}_p$, $\bar{C}_\infty = \varprojlim \bar{C}_n$, les limites projectives étant prises par rapport à la norme. Définissons $\tilde{C}_n$ comme étant l'image de l'homomorphisme naturel $\bar{C}_\infty \to \bar{C}_n$. Un argument de compacité standard montre que $\tilde{C}_n = \bigcap_{m \geq n} N_{F_m/F_n}(\bar{C}_m)$, d'où le nom de "normes universelles".

4.1. Théorème-définition. (voir [2], 2.2) *Le Λ-module $\bar{C}_\infty$ est libre (de rang $r = [F : \mathbb{Q}]$) si et seulement si les $\bar{C}_n$ vérifient la "descente galoisienne asymptotique" (DGA), i.e.*

$$\exists\, N \geq 0 \quad \textit{tel que} \quad \forall\, m \geq n \geq N,\ \bar{C}_m^{G_{m,n}} \simeq \bar{C}_n,\ \textit{avec} \quad G_{m,n} = \mathrm{Gal}(F_m/F_n)\,.$$

Modulo cette hypothèse (DGA), on va pouvoir calculer la G_n-cohomologie de C_n. Commençons par celle de $\tilde{C}_n$:

4.2. Lemme. *Sous (DGA), on a, pour tout $i \in \mathbb{Z}$:*

$$\hat{H}^i(G_n, \tilde{C}_n) \simeq \hat{H}^{i+1}(G_n, \mathbb{Z}_p^s) \simeq \begin{cases} 0 & \textit{si } i \textit{ est pair} \\ (\mathbb{Z}/p^n\mathbb{Z})^s & \textit{si } i \textit{ est impair} \end{cases}$$

Preuve. On sait que $\bar{U}'_\infty$ est Λ-libre de rang $r = [F : \mathbb{Q}]$ ([11], 7.2) et que l'homomorphisme naturel $(\bar{U}'_\infty)_{\Gamma_n} \to \bar{U}'_n$ est injectif pour tout $n \geq 0$ ([11], 7.3). Comme dans [2], 2.4, posons $Q_\infty = \bar{U}'_\infty/\bar{C}_\infty$ et écrivons la suite exacte de descente :

$$(\bar{U}'_\infty)^{\Gamma_n} = 0 \to (Q_\infty)^{\Gamma_n} \to (\bar{C}_\infty)_{\Gamma_n} \to (\bar{U}'_\infty)_{\Gamma_n} \hookrightarrow \bar{U}'_n\,.$$

Elle montre immédiatement que $(Q_\infty)^{\Gamma_n}$ s'identifie au noyau de l'homomorphisme canonique $(\bar{C}_\infty)_{\Gamma_n} \twoheadrightarrow \tilde{C}_n$. Par l'hypothèse (DGA), le $\mathbb{Z}_p[G_n]$-module $(\bar{C}_\infty)_{\Gamma_n}$ est libre, d'où $\hat{H}^i(G_n, \tilde{C}_n) \simeq \hat{H}^{i+1}(G_n, (Q_\infty)^{\Gamma_n})$. Il reste à calculer la G_n-cohomologie de $(Q_\infty)^{\Gamma_n}$. Passons à la limite projective (pour la norme) sur les suites exactes de valuation. Après passage au quotient par $\bar{C}_\infty$, nous obtenons une suite exacte de Λ-modules :

$$0 \to \bar{U}_\infty/\bar{C}_\infty \to \bar{U}'_\infty/\bar{C}_\infty \to \mathbb{Z}_p[S_\infty] \to D_\infty \to 0\,. \tag{3}$$

où $\mathbb{Z}_p[S_\infty] := \varprojlim \mathbb{Z}_p[S_n]$ est isomorphe à $\mathbb{Z}_p[S_0]$ par la norme (à cause de l'hypothèse de ramification (b)). Comme D_∞ est fini, la suite (3) peut se réécrire :

$$0 \to \bar{U}_\infty/\bar{C}_\infty \to Q_\infty \to \mathbb{Z}_p^s \to 0, \quad \text{avec action triviale de } \Gamma \text{ sur } \mathbb{Z}_p^s.$$

Par descente, on obtient :

$$0 \to (\bar{U}_\infty/\bar{C}_\infty)^{\Gamma_n} \to (Q_\infty)^{\Gamma_n} \to \mathbb{Z}_p^s \to (\bar{U}_\infty/\bar{C}_\infty)_{\Gamma_n}\,.$$

Par la Conjecture Principale (ou théorème de Mazur-Wiles), on sait que les Λ-modules $\bar{U}_\infty/\bar{C}_\infty$ et X_∞ ont même série caractéristique. La conjecture de Leopoldt en F_n entraîne alors la finitude de $(\bar{U}_\infty/\bar{C}_\infty)^{\Gamma_n}$ et de $(\bar{U}_\infty/\bar{C}_\infty)_{\Gamma_n}$. Mais on sait que $\bar{U}_\infty$ est Λ-libre ([2], 1.6), et $\bar{C}_\infty$ est Λ-libre par (DGA), donc le Λ-module $\bar{U}_\infty/\bar{C}_\infty$ est de dimension projective ≤ 1, ce qui équivaut à dire qu'il n'a pas de sous-module fini non nul. La suite exacte précédente donne alors un isomorphisme $(Q_\infty)^{\Gamma_n} \xrightarrow{\sim} \mathbb{Z}_p^s$, avec action triviale de Γ, ce qui détermine la démonstration du lemme. □

La clé qui permet de passer de $\tilde{C}_n$ à $\bar{C}_n$ est le résultat suivant de [2], dont la démonstration utilise essentiellement les relations de distribution que vérifient les unités circulaires :

4.3. Lemme. *Soit F^I le sous-corps d'inertie de $F/\mathbb{Q}$ en p. Notons $C(I) = C(F^I)$. Pour tout $n \geq 0$, le $\mathbb{Z}_p$-module $\bar{C}_n$ est engendré par $\tilde{C}_n$ et $\bar{C}(I)$.*

Preuve. Voir [2], lemme 2.5 ; si p est non ramifié dans F, voir [1], lemme 1.3. □

4.4. Corollaire. *La descente galoisienne asymptotique (DGA) entraîne la descente galoisienne (DG), i.e. :*

$$\forall\, m \geq n \geq 0\,, \quad \bar{C}_m^{G_{m,n}} \simeq \bar{C}_n\,.$$

Preuve. Tout $x \in \bar{C}_m$ s'écrit, d'après 4.3, sous la forme $x = yz$, avec $y \in \bar{C}(I)$ et $z \in \tilde{C}_m$. Tout générateur σ de $G_{m,n} = \mathrm{Gal}(F_m/F_n)$ fixe $\bar{C}(I)$, puisque $F^I \subseteq F$. Par suite, $(\sigma - 1) \cdot x = (\sigma - 1) \cdot z$, donc $z \in \tilde{C}_m^{G_{m,n}}$ si $x \in \bar{C}_m^{G_{m,n}}$. Or, d'après 4.2, $\tilde{C}_m^{G_{m,n}} = N_{F_m/F_n}(\tilde{C}_m) \subseteq \tilde{C}_n$, i.e. les $\tilde{C}_m$ vérifient la descente galoisienne. On en conclut que $\bar{C}_m^{G_{m,n}} \subseteq \bar{C}_n$. □

Dans la suite, en conséquence de 4.4, on se référera àl'hypothèse (DG) au lieu de (DGA).

Remarque. Si p est non ramifié dans F, l'hypothèse (HB) de [1] entraîne l'hypothèse (DG) ([1], 3.14). On ne connaît pas d'exemple de corps vérifiant (DG) sans vérifier (HB), bien qu'il semble peu probable que ces deux conditions soient équivalentes.

4.5. Lemme. *Sous (DG), tous les modules $\bar{C}_n/\tilde{C}_n$ sont isomorphes à $\Phi := \bar{C}_0/\tilde{C}_0$, qui est un module Γ-trivial, de $\mathbb{Z}_p$-rang égal à $(s-1)$.*

Preuve. D'après le lemme 4.3, $\bar{C}_n/\tilde{C}_n \simeq \bar{C}(I)/\bar{C}(I) \cap \tilde{C}_n$. Il suffit donc de montrer que tous les $\bar{C}(I) \cap \tilde{C}_n$ sont égaux à $\bar{C}(I) \cap \tilde{C}_0$. On a une inclusion évidente $\bar{C}(I) \cap \tilde{C}_0 \subseteq \bar{C}(I) \cap \tilde{C}_n$. En sens inverse, on a $\bar{C}(I) \cap \tilde{C}_n \subseteq \tilde{C}_n^{G_n}$ (puisque $F^I \subseteq F$), et $\tilde{C}_n^{G_n} = N_{F_n/F}(\tilde{C}_n)$ d'après 4.2, d'où finalement $\bar{C}(I) \cap \tilde{C}_n \subseteq \bar{C}(I) \cap \tilde{C}_0$, ce qui montre la première partie du lemme. Il reste à calculer le $\mathbb{Z}_p$-rang de Φ. Or $\mathrm{rang}_{\mathbb{Z}_p} \bar{C}_0 = (r-1)$, et $\mathrm{rang}_{\mathbb{Z}_p} \tilde{C}_0 = \mathrm{rang}_{\mathbb{Z}_p} (\bar{C}_\infty)_\Gamma - \mathrm{rang}_{\mathbb{Z}_p} (Q_\infty)^\Gamma = r - s$ d'après les calculs de 4.2. □

Dans toute la suite, on notera $t\Phi$ la $\mathbb{Z}_p$-torsion de Φ, de sorte que $\Phi \simeq t\Phi \oplus \mathbb{Z}_p^{s-1}$, avec action triviale de Γ. On peut maintenant calculer la G_n-cohomologie de C_n en fonction de $t\Phi$:

4.6. Théorème. (cp. [1], 3.15) *Sous (DG), pour tout $n \geq 0$, on a un isomorphisme : $\hat{H}^0(G_n, C_n) \xrightarrow{\sim} (t\Phi/p^n) \oplus (\mathbb{Z}/p^n\mathbb{Z})^{s-1}$ et une suite exacte : $0 \to (\mathbb{Z}/p^n\mathbb{Z})^s \to H^1(G_n, C_n) \to (t\Phi)[p^n] \to 0$.*

Preuve. De la suite exacte tautologique $0 \to \tilde{C}_n \to \bar{C}_n \to \Phi \to 0$, on tire l'hexagone exact de cohomologie :

$$\begin{array}{ccccc}
\hat{H}^0(G_n, \tilde{C}_n) & \longrightarrow & \hat{H}^0(G_n, \bar{C}_n) & \longrightarrow & \hat{H}^0(G_n, \Phi) \\
\uparrow & & & & \downarrow \\
\hat{H}^{-1}(G_n, \Phi) & \longleftarrow & \hat{H}^{-1}(G_n, \bar{C}_n) & \xleftarrow{\varphi} & \hat{H}^{-1}(G_n, \tilde{C}_n)
\end{array}$$

Or, d'après 4.3, pour tout générateur σ de G_n, on a : $(\sigma - 1)\, \bar{C}_n = (\sigma - 1)\, \tilde{C}_n$ (puisque σ fixe $\bar{C}(I)$), ce qui montre que l'homomorphisme φ est injectif, d'où deux suites exactes :

$$\hat{H}^0(G_n, \tilde{C}_n) = 0 \to \hat{H}^0(G_n, \bar{C}_n) \to \hat{H}^0(G_n, \Phi) \simeq (t\Phi/p^n) \oplus (\mathbb{Z}/p^n\mathbb{Z})^{s-1} \to 0$$

et (en tenant compte de la cyclicité de G_n)

$$0 \to H^1(G_n, \tilde{C}_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^s \to H^1(G_n, \bar{C}_n) \to H^1(G_n, \Phi) \simeq (t\Phi)[p^n] \to 0\,.$$

□

Remarque. Les résultats énoncés dans le théorème 4.6 deviennent particulièrement simples si $t\Phi$ est trivial. *C'est ce qui se produit dans le cas p-décomposé* : en effet, dans ce cas, il est connu (et l'on y reviendra en 5.5 ci-dessous) que les normes universelles sont triviales, et donc $\Phi = \bar{C}_0$ est sans $\mathbb{Z}_p$-torsion.

4.7. Corollaire. *Sous (DG), on a un isomorphisme de modules galoisiens :* $H^2(\Gamma, C_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{s-1}$ *et un isomorphisme de groupes abéliens :* $H^1(\Gamma, C_\infty) \simeq (t\Phi) \oplus (\mathbb{Q}_p/\mathbb{Z}_p)^s$.

Preuve. Par passage à la limite inductive sur l'inflation, on obtient évidemment une suite exacte : $0 \to (\mathbb{Q}_p/\mathbb{Z}_p)^s) \to H^1(\Gamma, C_\infty) \to t\Phi \to 0$, d'où l'isomorphisme de groupes abéliens annoncé. Concernant H^2, si l'on identifie $H^2(G_n, C_n)$ à $\hat{H}^0(G_n, C_n)$ par cyclicité, l'inflation $H^2(G_n, C_n) \to H^2(G_{n+1}, C_{n+1})$ se traduit par la multiplication par p : $(t\Phi/p^n) \oplus (\mathbb{Z}/p^n\mathbb{Z})^s \xrightarrow{p} (t\Phi/p^{n+1}) \oplus (\mathbb{Z}/p^{n+1}\mathbb{Z})^s$, d'où l'isomorphisme de modules annoncé. □

5 Unités modulo unités circulaires

Le corps de base F vérifie les mêmes hypothèses que dans le §3. On se propose d'étudier la descente galoisienne sur les modules $B_n := \bar{U}_n/\bar{C}_n$. L'ordre de B_n est contrôlé par la *formule d'indice de Sinnott :*

$(U_n : C_n)$ "=" $c_n\, h_n$ (à une puissance de 2 près), où h_n est le nombre de classes de F_n et $c_n = c(F_n)$ est un nombre rationnel, *borné* uniformément en n ([14] ; voir aussi le résumé de la section 2.2 de [4]). Pour contrôler la descente, on introduit les modules $B_\infty := \varinjlim B_n$ (limite inductive pour les applications induites par l'inclusion) et $Y_\infty := \varprojlim B_n$ (limite projective pour la norme). Le point-clé est le résultat technique suivant :

5.1. Proposition. *Les groupes* $H^0(\Gamma, B_\infty)$ *et* $H^1(\Gamma, B_\infty)$ *sont finis.*

Remarque. Ce résultat a été "démontré" par Kim & Oh dans le cas particulier où F est un corps quadratique réel p-décomposé. Mais dans [12], p. 170, les auteurs affirment que la finitude de $(B_\infty)^\Gamma$ provient de [15], lemme 15.39 et proposition 15.44, alors que dans [15], le corps de base est un sous-corps de $\mathbb{Q}(\xi_p)$! De plus, on sait que si les unités circulaires de Sinnott coïncident avec celles de Washington pour les corps cyclotomiques, elles ne coïncident pas en général : une condition nécessaire et suffisante de coïncidence est justement l'hypothèse (DGA) ([2], proposition 3.6). La technicité de la démonstration qui va suivre, et qui semble inhérente au problème, jette un doute supplémentaire sur la référence cryptique de [12].

Preuve. Le principe de la preuve consiste à comparer les deux systèmes $((Y_\infty)_{\Gamma_n})_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$, dont on va montrer qu'ils sont *uniformément pseudo-isomorphes* au sens suivant : pour tout $n \geq 0$, l'homomorphisme naturel $(Y_\infty)_{\Gamma_n} \to B_n$ a un noyau et un conoyau finis, bornés uniformément en n. Procédons en deux étapes :

1) Pour tout $n \geq 0$, notons $\tilde{U}_n$ l'image de l'homomorphisme naturel $\bar{U}_\infty \to \bar{U}_n$, et montrons que les deux systèmes $((Y_\infty)_{\Gamma_n})_{n\in\mathbb{N}}$ et $(\tilde{U}_n/\tilde{C}_n)_{n\in\mathbb{N}}$ sont uniformément pseudo-isomorphes. La suite exacte tautologique $0 \to \bar{C}_\infty \to \bar{U}_\infty \to Y_\infty \to 0$ donne par cohomologie une suite exacte $(\bar{U}_\infty)^{\Gamma_n} = 0 \to (Y_\infty)^{\Gamma_n} \to (\bar{C}_\infty)_{\Gamma_n} \xrightarrow{\alpha_n} (\bar{U}_\infty)_{\Gamma_n} \to (Y_\infty)_{\Gamma_n} \to 0$. On peut donc remplacer $(Y_\infty)_{\Gamma_n}$ par coker α_n et comparer les systèmes $(\operatorname{coker}\alpha_n)_{n\in\mathbb{N}}$ et $(\tilde{U}_n/\tilde{C}_n)_{n\in\mathbb{N}}$. On a un diagramme commutatif aux lignes exactes :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\bar{U}'_\infty/\bar{C}_\infty)^{\Gamma_n} & \longrightarrow & (\bar{C}_\infty)_{\Gamma_n} & \longrightarrow & \tilde{C}_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta_n} & & \downarrow{\scriptstyle \alpha_n} & & \cap & & \\
0 & \longrightarrow & (\bar{U}'_\infty/\bar{U}_\infty)^{\Gamma_n} & \longrightarrow & (\bar{U}_\infty)_{\Gamma_n} & \longrightarrow & \tilde{U}_n & \longrightarrow & 0
\end{array}$$

La ligne exacte du haut a été construite dans la démonstration du lemme 4.2. La ligne exacte du bas se construit exactement de même, en remplaçant $\bar{C}_\infty$ par $\bar{U}_\infty$. Le lemme du serpent donne immédiatement une suite exacte :

$$0 \to \operatorname{coker}\beta_n \to \operatorname{coker}\alpha_n \to \tilde{U}_n/\tilde{C}_n \to 0\,.$$

On a vu dans la démonstration de 4.2 que la Conjecture Principale et la conjecture de Leopoldt pour F_n entraînent la finitude de $(Y_\infty)_{\Gamma_n}$, donc coker β_n est aussi fini. Comme coker β_n se stabilise évidemment par nœtherianité, on a bien montré que les systèmes $(\operatorname{coker}\alpha_n)_{n\in\mathbb{N}}$ et $(\tilde{U}_n/\tilde{C}_n)_{n\in\mathbb{N}}$ sont uniformément pseudo-isomorphes.

2) Comparons maintenant les deux systèmes $(\tilde{U}_n/\tilde{C}_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$. Pour tout $n \geq 0$, notons f_n l'homomorphisme naturel $\tilde{U}_n/\tilde{C}_n \to \bar{U}_n/\bar{C}_n = B_n$. Il suffit de montrer que ker f_n est borné : en effet, on a vu dans la première étape que les systèmes $\tilde{U}_n/\tilde{C}_n$ et $(Y_\infty)_{\Gamma_n}$ ont les mêmes invariants λ et μ, qui sont ceux de la série caractéristique de Y_∞, et la formule d'indice de Sinnott implique que les systèmes B_n et A_n ont les mêmes invariants λ et μ, qui sont ceux de la série caractéristique de X_∞ ; or X_∞ et Y_∞ ont même série caractéristique d'après

la Conjecture Principale. Pour borner $\ker f_n$, notons que ce noyau est égal à $(\tilde{U}_n \cap \bar{C}_n)/\tilde{C}_n$, d'où une suite exacte : $0 \to \ker f_n \to \bar{C}_n/\tilde{C}_n \to \bar{U}_n/\tilde{U}_n$. Comme $\ker f_n$ est fini, il s'injecte dans le module de torsion de $\bar{C}_n/\tilde{C}_n$. Or, d'après 4.3, on a une surjection naturelle $\bar{C}_0/\tilde{C}_0 \simeq \bar{C}(I)/\bar{C}(I) \cap \tilde{C}_0 \twoheadrightarrow \bar{C}_n/\tilde{C}_n \simeq \bar{C}(I)/\bar{C}(I) \cap \tilde{C}_n$, dont le noyau est fini puisque $\bar{C}_0/\tilde{C}_0$ et $\bar{C}_n/\tilde{C}_n$ ont même $\mathbb{Z}_p$-rang égal à $(s-1)$. Il s'ensuit que la torsion de $\bar{C}_n/\tilde{C}_n$ est un quotient de la torsion de $\bar{C}_0/\tilde{C}_0$, ce qui montre bien que $\ker f_n$ est borné.

Pour terminer la démonstration de la proposition, introduisons le module $\mathcal{B}_\infty := \varinjlim (Y_\infty)_{\Gamma_n}$. D'après ce qu'on vient de voir, il suffit de montrer la finitude de $H^0(\Gamma, \mathcal{B}_\infty)$ et $H^1(\Gamma, \mathcal{B}_\infty)$. Or, comme les $(Y_\infty)_{\Gamma_n}$ sont finis par Leopoldt, la théorie de l'adjoint d'Iwasawa s'applique ([9], [15], ...), qui donne un isomorphisme $\mathcal{B}_\infty \simeq \mathrm{Hom}(\alpha(Y_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$, où $\alpha(\cdot)$ désigne l'adjoint. Comme $H^0(\Gamma, \mathcal{B}_\infty) = (\mathcal{B}_\infty)^\Gamma$ et $H^1(\Gamma, \mathcal{B}_\infty) = (\mathcal{B}_\infty)_\Gamma$ (car $\mathcal{B}_\infty$ est un groupe abélien de torsion), le problème revient, par dualité, à montrer la finitude de $\alpha(Y_\infty)^\Gamma$ et $\alpha(Y_\infty)_\Gamma$, c'est-à-dire par exemple la finitude de $\alpha(Y_\infty)^\Gamma$, puisque cet adjoint est un Λ-module de torsion. Mais, de façon générale, $\alpha(Y_\infty)$ est pseudo-isomorphe à $Y_\infty^{\#}$, où le signe # signifie qu'on a inversé l'action de Γ. La finitude de $(Y_\infty^{\#})^\Gamma$ est équivalente à celle de $(Y_\infty)^\Gamma$, qui provient de la Conjecture Principale et de la conjecture de Leopoldt. □

On va maintenant s'approcher de la descente galoisienne sur les B_n, par une suite de lemmes dont les hypothèses, malheureusement, seront de plus en plus restrictives.

5.2. Lemme. *Supposons que $X_\infty^0 = (0)$. Alors l'homomorphisme naturel $H^1(\Gamma, C_\infty) \to H^1(\Gamma, U_\infty)$ est surjectif.*

Preuve. La suite exacte tautologique $0 \to C_\infty \to U_\infty \to U_\infty/C_\infty \to 0$ donne, par cohomologie, une suite exacte $\to H^1(\Gamma, C_\infty) \to H^1(\Gamma, U_\infty) \to H^1(\Gamma, U_\infty/C_\infty)$. Si $X_\infty^0 = (0)$, le corollaire 3.2 montre que $H^1(\Gamma, U_\infty)$ est isomorphe à $(\mathbb{Q}_p/\mathbb{Z}_p)^s$, donc n'a pas de quotient fini non nul. Or $H^1(\Gamma, U_\infty/C_\infty) = \varinjlim H^1(G_n, U_n/C_n) = \varinjlim H^1(G_n, B_n) = H^1(\Gamma, B_\infty)$, qui est fini d'après 5.1. Cela démontre la surjectivité annoncée. □

5.3. Lemme. *Sous (DG), supposons en outre que $X_\infty^0 = (0)$ et $t\Phi = (0)$. Alors, pour tout $n \geq 0$, $B_0 \xrightarrow{\sim} (B_n)^{G_n}$ et l'homomorphisme naturel $H^1(G_n, C_n) \to H^1(G_n, U_n)$ est un isomorphisme.*

Preuve. La suite exacte tautologique $0 \to \bar{C}_n \to \bar{U}_n \to B_n \to 0$ donne, par cohomologie et sous (DG), une suite exacte :

$$0 \to B_0 \to (B_n)^{G_n} \to H^1(G_n, C_n) \xrightarrow{\text{nat}} H^1(G_n, U_n) \xrightarrow{g_n} H^1(G_n, B_n)\,. \qquad (4)$$

Sous les hypothèses du lemme, montrons que l'homomorphisme g_n est nul. Pour cela, considérons le diagramme commutatif (où les flèches verticales sont données par l'inflation) :

$$\begin{array}{ccccccc}
\longrightarrow & H^1(G_n, U_n) & \xrightarrow{g_n} & H^1(G_n, B_n) & \longrightarrow & H^2(G_n, C_n) \\
& \big\downarrow & & \big\downarrow \mathrm{inf}_1 & & \big\downarrow \mathrm{inf}_2 \\
\longrightarrow & H^1(\Gamma, U_\infty) & \xrightarrow{g_\infty} & H^1(\Gamma, B_\infty) & \longrightarrow & H^2(\Gamma, C_\infty)
\end{array}$$

La première flèche verticale est injective, puisque $U_\infty^{\Gamma_n} = U_n$. Sous (DG) et modulo la nullité de $t\Phi$, on a vu en 4.7 que $H^2(G_n, C_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{s-1}$ s'injecte par inflation dans $H^2(\Gamma, C_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{s-1}$. On en déduit l'injectivité de inf_1. Or l'homomorphisme g_∞ est nul d'après 5.2, d'où la nullité de g_n, i.e. la surjectivité de $H^1(G_n, C_n) \xrightarrow{\text{nat}} H^1(G_n, U_n)$. Comme ces deux groupes sont isomorphes à $(\mathbb{Z}/p^n\mathbb{Z})^s$ d'après 3.2 (par nullité de X_∞^0) et 4.6 (par nullité de $t\Phi$), l'homomorphisme naturel est un isomorphisme. On en déduit aussi l'isomorphisme $B_0 \xrightarrow{\sim} (B_n)^{G_n}$. $\square$

5.4. Lemme. *Gardons les hypothèses du lemme 5.3, et supposons en outre que la constante de Sinnott $c(F)$ est une p-unité. Alors, pour tout $n \geq 0$, l'homomorphisme naturel $H^2(G_n, C_n) \to H^2(G_n, U_n)$ est un isomorphisme, et $H^1(G_n, B_n) = H^2(G_n, B_n) = 0$.*

Remarque. La constante de Sinnott $c(F)$ peut s'écrire comme un produit de deux facteurs $c'(F) \cdot c''(F)$, l'un de type "galoisien", l'autre de type arithmétique. Plus précisément, $c'(F) = \prod_\ell [F \cap \mathbb{Q}(\xi_{\ell^\infty}) : \mathbb{Q}]/[F : \mathbb{Q}]$, et $c''(F)$ est l'indice généralisé $(\mathbb{Z}[G] : Iw(F))$, où $G = \mathrm{Gal}(F/\mathbb{Q})$ et $Iw(F)$ est un certain sous-module de $\mathbb{Q}[G]$ dont Sinnott attribue la paternité à Iwasawa (voir [14]). La p-partie de $c(F)$ est triviale dans un grand nombre de cas "usuels", en particulier *dans le cas semi-simple.*

Preuve. D'après 5.3, $H^1(G_n, C_n) \overset{\text{nat}}{\xrightarrow{\sim}} H^1(G_n, U_n)$ et la suite exacte de cohomologie (4) se continue ainsi :

$$0 \to H^1(G_n, B_n) \to H^2(G_n, C_n) \xrightarrow{\text{nat}} H^2(G_n, U_n) \to H^2(G_n, B_n)\,. \qquad (5)$$

Montrons la nullité de $H^i(G_n, B_n)$ pour $i = 1, 2$. Dans la preuve de la proposition 5.1, on a vu que le dual de Pontryagin $\check{B}_\infty$ de B_∞ est pseudo-isomorphe à $Y_\infty^\#$, et Y_∞ et X_∞ ont la même série caractéristique, disons $H(T)$. On en déduit l'égalité des Γ-quotients de Herbrand :

$$|(\check{B}_\infty)_\Gamma|/|(\check{B}_\infty)^\Gamma| = |(X_\infty)_\Gamma|/|(X_\infty)^\Gamma| \sim H(0)\,,$$

où le signe $\sim$ signifie l'égalité à une unité p-adique près. Par hypothèse, $(X_\infty^0)^\Gamma = (X_\infty)^\Gamma = (0)$ et la relation précédente peut se réécrire : $|H^0(\Gamma, B_\infty)|/|H^1(\Gamma, B_\infty)| = |(X_\infty)_\Gamma|$. D'après 5.3, $(B_\infty)^\Gamma = B_0$, dont l'ordre est égal à celui de A_0, puisqu'on a supposé que la constante de Sinnott est une unité p-adique.

Or $(X_\infty)_\Gamma \twoheadrightarrow A_0$ canoniquement, donc la relation précédente implique la trivialité de $H^1(\Gamma, B_\infty)$, et par suite la trivialité de $H^1(G_n, B_n)$ (par (DG) ou par l'injectivité de $\inf_1$ dans la preuve de 5.3). Comme B_n est fini, son G_n-quotient de Herbrand est trivial, d'où la trivialité de $H^2(G_n, B_n)$ également. On déduit alors de (5) que l'homomorphisme $H^2(G_n, C_n) \xrightarrow{\text{nat}} H^2(G_n, U_n)$ est un isomorphisme. $\square$

On peut maintenant démontrer le théorème principal énoncé dans l'introduction :

5.5. Théorème. *Soit F un corps abélien réel tel que $p \nmid [F : \mathbb{Q}]$ et p se décompose totalement dans F. Alors $X_\infty(F)$ est nul si et seulement si son sous-module fini maximal $X^0_\infty(F)$ est nul.*

Preuve. On a déjà signalé que l'hypothèse de semi-simplicité ($p \nmid [F : \mathbb{Q}]$) entraîne que la constante de Sinnott $c(F)$ est une unité p-adique (remarque suivant 5.4). Elle entraîne aussi la condition (HB), donc la condition (DGA) (voir le début du §4). Quant à l'hypothèse de p-décomposition, il est bien connu qu'elle entraîne la trivialité des normes universelles $\tilde{U}_0$ (voir e.g. [5], 1.1), donc aussi la trivialité de $\tilde{C}_0$, et par conséquent la $\mathbb{Z}_p$-liberté de $\Phi = \bar{C}_0/\tilde{C}_0 = \bar{C}_0$.

Supposons maintenant que $X^0_\infty = (0)$. Toutes les hypothèses du lemme 5.4 sont vérifiées. Pour montrer la nullité de X_∞, revenons à l'étape 2) de la preuve de la proposition 5.1. En notant f_n l'homomorphisme canonique $\tilde{U}_n/\tilde{C}_n \to \bar{U}_n/\bar{C}_n$, on a évidemment une suite exacte

$$0 \to \ker f_n \to \bar{C}_n/\tilde{C}_n \to \bar{U}_n/\tilde{U}_n \to \operatorname{coker} f_n \to 0\,.$$

Comme $\ker f_n$ est fini et $\bar{C}_n/\tilde{C}_n \simeq \Phi$, la nullité de $t\Phi$ entraîne celle de $\ker f_n$. Posons $Q_n = \operatorname{coker} f_n$ et considérons le diagramme commutatif (où les flèches verticales sont induites par la norme) :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bar{C}_n/\tilde{C}_n & \longrightarrow & \bar{U}_n/\tilde{U}_n & \longrightarrow & Q_n & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle \nu_C} & & \big\downarrow{\scriptstyle \nu_U} & & \big\downarrow{\scriptstyle \nu_Q} & & \\ 0 & \longrightarrow & \bar{C}_0 & \longrightarrow & \bar{U}_0 & \longrightarrow & Q_0 = \bar{U}_0/\bar{C}_0 & \longrightarrow & 0 \end{array} \qquad (6)$$

Comme G_n opère trivialement sur $\Phi \simeq \bar{C}_n/\tilde{C}_n$, ν_C s'identifie à la multiplication par p^n, et donc $\ker \nu_C = (0)$. Passons à $\ker \nu_U$. Pour tout $n \geq 0$, notons $\mathcal{U}_n$ le produit, pour toutes les p-places v de F_n, des unités locales principales $\bar{U}_{n,v}$.

La suite exacte du corps de classes relative à l'inertie s'écrit, au niveau de F_n :

$$\begin{tikzcd}
0 \arrow[r] & \bar{U}_n \arrow[r] & \mathcal{U}_n \arrow[r, "\text{Artin}"] \arrow[dr, hook] & \mathcal{X}_n \arrow[r] & A_n \arrow[r] & 0 \\
 & & & I_n \arrow[u, two heads] & &
\end{tikzcd}$$

(l'exactitude à gauche provient de la conjecture de Leopoldt pour F_n). En passant à la limite projective sur la norme, on obtient une suite exacte analogue au niveau infini, d'où, par descente, un diagramme commutatif :

$$\begin{tikzcd}
(I_\infty)^{\Gamma_n} \arrow[r] & (\bar{U}_\infty)_{\Gamma_n} \arrow[r] \arrow[d] & (\mathcal{U}_\infty)_{\Gamma_n} \arrow[r] \arrow[d] & (I_\infty)_{\Gamma_n} \arrow[r] \arrow[d, "\delta_n"] & 0 \\
0 \arrow[r] & \bar{U}_n \arrow[r] & \mathcal{U}_n \arrow[r] & I_n \arrow[r] & 0
\end{tikzcd}$$

Ici, $\varprojlim I_n := I_\infty \subset \mathcal{X}_\infty$, et $(I_\infty)^{\Gamma_n} = (0)$ puisque $(\mathcal{X}_\infty)^{\Gamma_n} = (0)$ par la conjecture de Leopoldt. Le lemme du serpent appliqué au diagramme précédent donne un autre diagramme commutatif (avec une notation évidente pour $\tilde{\mathcal{U}}_n$) :

$$\begin{tikzcd}
\arrow[r] & \ker \delta_n \arrow[r] & \bar{U}_n/\tilde{U}_n \arrow[r] \arrow[d, "\nu_U"] & \mathcal{U}_n/\tilde{\mathcal{U}}_n \arrow[r] \arrow[d, "\nu_{\mathcal{U}}"] & {} \\
 & 0 \arrow[r] & \bar{U}_0/\tilde{U}_0 \arrow[r] & \mathcal{U}_0/\tilde{\mathcal{U}}_0 \arrow[r] & {}
\end{tikzcd}$$

Les flèches verticales sont induites par la norme. La flèche $\nu_{\mathcal{U}}$ est facilement décrite par le corps de classes local, puisque, pour toute p-place v, $\bar{U}_{n,v}/\tilde{U}_{n,v}$ est isomorphe (en tenant compte de l'hypothèse de ramification (b)) au groupe de Galois de la $\mathbb{Z}_p$-extension cyclotomique de $F_{n,v}$. Il en résulte en particulier que l'application $\nu_{\mathcal{U}}$ est injective, d'où, par chasse dans le diagramme, une surjection $\ker \delta_n \twoheadrightarrow \ker \nu_U$.

Il reste à déterminer $\ker \delta_n$, ce qui se fait en examinant la seconde partie des suites exactes du corps de classes :

$$\begin{tikzcd}
0 \arrow[r] & (X_\infty)^{\Gamma_n} \arrow[r] & (I_\infty)_{\Gamma_n} \arrow[r] \arrow[d, "\delta_n"] & (\mathcal{X}_\infty)_{\Gamma_n} \arrow[r] \arrow[d] & (X_\infty)_{\Gamma_n} \arrow[r] \arrow[d] & 0 \\
 & 0 \arrow[r] & I_n \arrow[r] & \mathcal{X}_n \arrow[r] & X_n \arrow[r] & 0
\end{tikzcd}$$

Par la conjecture de Leopoldt pour F_n, on sait que $(\mathcal{X}_\infty)_{\Gamma_n} \simeq \mathrm{tor}_{\mathbb{Z}_p}\mathcal{X}_n$, d'où $(X_\infty)^{\Gamma_n} \xrightarrow{\sim} \ker \delta_n$. Par l'hypothèse de trivialité de X_∞^0, on en déduit la trivialité de $\ker \nu_U$.

(NB : dans cette partie de la démonstration, on n'a pas utilisé l'hypothèse de p-décomposition.)

Revenons au diagramme (6) qui nous donne, par le lemme du serpent, une suite exacte :

$$\ker \nu_U = 0 \to \ker \nu_Q \to \operatorname{coker} \nu_C \simeq \hat{H}^0(G_n, C_n) \to \operatorname{coker} \nu_U \simeq \hat{H}^0(G_n, U_n)$$

$$\to \operatorname{coker} \nu_Q \to 0\,.$$

D'après 5.4, l'application naturelle $\hat{H}^0(G_n, C_n) \to \hat{H}^0(G_n, U_n)$ est un isomorphisme, d'où la nullité de $\ker \nu_Q$ et $\mathrm{coker}\nu_Q$. Autrement dit, pour tout $n \geq 0$, la norme induit un isomorphisme $Q_n \xrightarrow{\sim} Q_0 = \bar{U}_0/\bar{C}_0 = B_0$. Mais par définition même des normes universelles, $\varprojlim \bar{U}_n/\tilde{U}_n = (0)$, d'où $\varprojlim Q_n = (0)$, et donc $B_0 = (0)$. Or l'on a vu dans la preuve du lemme 5.3 que $|(X_\infty)_\Gamma| = |(B_\infty)^\Gamma| = |B_0|$, d'où la nullité cherchée de X_∞. $\square$

5.6. Corollaire. *Sous les hypothèses du théorème, le couple (F, p) vérifie la conjecture de Greenberg faible.*

En fait, la condition de semi-simplicité dans 5.5 et 5.6 a seulement servi à assurer la validité de deux propriétés (voir le début de la preuve de 5.5) : l'hypothèse (HB) et la p-trivialité de la constante de Sinnott $c(F)$, d'où l'on a déduit (en supposant $X^0_\infty = (0)$) la p-principalité de F, i.e. la trivialité de A_F (fin de la preuve de 5.5). Inversement, on sait que la p-principalité de F entraîne l'hypothèse (HB) et la p-trivialité de $c(F)$; l'argument de 5.4 montre alors la nullité de B_∞. Autrement dit :

5.7. Théorème. *Soit F un corps abélien réel, p-décomposé, p-principal. Alors le couple (F, p) vérifie la conjecture (GF).*

Remerciements. Ce travail a été effectué pendant un séjour (de mars à août 2005) à l'IHÉS que je remercie pour son hospitalité. Je tiens également à remercier J.-R. Belliard pour de nombreuses et utiles discussions sur la cohomologie des unités circulaires.

Références

[1] J.-R. Belliard, Sur la structure galoisienne des unités circulaires dans les $\mathbb{Z}_p$-extensions, *J. Number Theory*, **69**, 1 (1998), 16-49.

[2] J.-R. Belliard, Sous-modules d'unités en théorie d'Iwasawa, *Publ. Math. Besançon, Théorie des Nombres* (2002), 12 pages.

[3] R. Badino, T. Nguyen Quang Do, Sur les égalités du miroir et certaines formes faibles de la conjecture de Greenberg, *Manuscripta Math.*, **116** (2005), 323-340.

[4] J.-R. Belliard, T. Nguyen Quang Do, Formules de classes pour les corps abéliens réels, *Ann. Inst. Fourier*, **51**, 4 (2001), 903-937.

[5] J.-R. Belliard, T. Nguyen Quang Do, On modified circular units and annihilation of real classes, *Nagoya Math. J.*, **177** (2005), 77-115.

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

[7] R. Greenberg, Iwasawa theory, past and present, *Adv. Studies in Pure Math.*, **30** (2001), "Class Field Theory – Its centenary and prospect", 335-385.

[8] H. Ichimura, A note on the λ-invariant of real quadratic fields, *Proc. Japan Acad. Ser. A Math. Sci.*, **72**, 1 (1996), 28-30.

[9] K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, *Ann. of Math.*, **98** (1973), 246-326.

[10] K. Iwasawa, On cohomology groups of units for $\mathbb{Z}_p$-extensions, *Amer. J. Math.*, **105** (1982), 189-200.

[11] L.V. Kuz'min, The Tate module for algebraic number fields, *Math. USSR Izv.*, **6**, 2 (1972), 263-321.

[12] J.M. Kim, S.I. Oh, On the Iwasawa λ-invariants of real quadratic fields, *Acta Arithm.*, XCVI, 2 (2000), 167-174.

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

[14] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, *Invent. Math.*, **62**, 2 (1980), 181-234.

[15] L. Washington, "Introduction to cyclotomic fields", Springer GTM, 2$^{\text{nd}}$ edition, New-York (1997).

[16] K. Wingberg, Duality theorems for Γ-extensions of algebraic number fields, *Compos. Math.*, **55** (1985), 333-381.

T. Nguyen Quang Do
nguyen@math.univ-fcomte.fr