



**Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation
ESA - CNRS 6090**

Généralisation du Lemme de Kummer

Jilali Assim & Thong Nguyeb Quang Do

Rapport de recherche n° 2003-05

Université de Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex
Tél. 05 55 45 73 23 - Fax. 05 55 45 73 22 - laco@unilim.fr

<http://www.unilim.fr/laco/>

Généralisations Du Lemme De Kummer

Jilali Assim et Thong Nguyen Quang Do

Abstract

Kummer's lemma for the cyclotomic field $\mathbb{Q}(\mu_p)$ gives sufficient local conditions for a unit to be a global p -th power, and can thus be viewed as an early version of Leopoldt's conjecture. To study generalizations and converse statements, we introduce the "Kummer constant" $\kappa(F)$ of a number field F and compute it in Iwasawa theoretic terms. The vanishing of $\kappa(F)$ gives the desired generalization and converse of Kummer's lemma.

Introduction. Soit p un nombre premier impair et soit μ_p le groupe des racines p -ièmes de l'unité. Le célèbre lemme de Kummer (1847) pour le corps cyclotomique $K = \mathbb{Q}(\mu_p)$, est l'une des étapes-clés de la démonstration par Kummer du théorème de Fermat pour les exposants premiers réguliers. Il s'énonce ainsi :

Lemme de Kummer (voir [W3] Theorem 5.36). *Si le nombre premier p est régulier, le corps cyclotomique $K = \mathbb{Q}(\mu_p)$ vérifie la propriété :*

(\mathcal{K}) *Toute unité u de $K = \mathbb{Q}(\mu_p)$ congrue à un entier de \mathbb{Z} modulo p est puissance p -ième d'une unité de K .*

Deux questions se posent naturellement, qu'on va examiner dans l'ordre inverse de l'ordre chronologique :

- (i) Donner une réciproque du lemme de Kummer,
- (ii) Généraliser le lemme à un corps de nombres quelconque.

Concernant (i), un examen attentif de la démonstration du théorème 5.36 de [W3] montre que la seule hypothèse utilisée est la non-divisibilité par p du quotient $R_p(K^+)/\sqrt{|D(K^+)|}$, où K^+ est le sous-corps réel maximal de K , $R_p(K^+)$ est le régulateur p -adique de K^+ et $D(K^+)$ son discriminant. Compte tenu de cette observation, le problème (i) a été résolu pour $K = \mathbb{Q}(\mu_p)$ par B. Anglès :

$$(\mathcal{K}) \iff R_p(K^+)/\sqrt{|D(K^+)|} \sim 1$$

où \sim désigne l'égalité à une unité p -adique près ([A], th. 6.5). La démonstration de [A] utilise les lois de réciprocité explicites et les unités cyclotomiques de $\mathbb{Q}(\mu_p)$, et ne peut donc pas se généraliser à un corps de nombres quelconque. D'ailleurs, le résultat lui-même ne se généralise pas (voir théorème 2 et corollaire 4 ci-dessous).

Pour le problème (ii), il faut commencer par reformuler l'hypothèse du lemme de Kummer sur les unités de $\mathbb{Q}(\mu_p)$ en la plaçant dans le cadre de la conjecture de Leopoldt. En effet, il est bien connu ([W3] pages 80-81) qu'une unité de $\mathbb{Q}(\mu_p)$ est congrue à un entier de \mathbb{Z} modulo p si et seulement si elle est puissance p -ième locale en la place divisant p . À ce titre, le lemme de Kummer apparaît comme une version précoce de la conjecture de Leopoldt, qui peut s'énoncer ainsi pour un corps de nombres quelconque F :

$$(\mathcal{L}) \quad \exists c = c(F) / \forall n \gg 0, \forall u \in U_F, (u \in F_v^{p^{n+c}}, \forall v \mid p) \Rightarrow u \in U_F^{p^n}$$

où U_F est le groupe des unités de F et pour tout $v \mid p$, F_v est le complété de F en la place v (proposition 1). Si F vérifie la conjecture de Leopoldt en p , on appellera *constante de Kummer* de F , notée $\kappa(F)$, la valeur minimale des constantes $c(F)$ intervenant dans la propriété (\mathcal{L}) . Le lemme de Kummer donne alors une condition suffisante pour que la constante de Kummer de $\mathbb{Q}(\mu_p)$ soit nulle. Dans cet ordre d'idées, il a été généralisé par divers auteurs qui ont traité des corps cyclotomiques $\mathbb{Q}(\mu_{p^n})$ ([W1], [W2]), ou d'un corps de nombres totalement réel et des étages de sa \mathbb{Z}_p -extension cyclotomique ([O]), et qui majorent la constante de Kummer de ces corps par des valeurs spéciales de fonctions L p -adiques ou, ce qui revient au même à cause de la Conjecture Principale de la théorie d'Iwasawa, par les ordres de certains modules d'Iwasawa.

Dans le présent article, nous nous proposons, pour un corps de nombres F quelconque vérifiant la conjecture de Leopoldt, de donner la valeur exacte de $\kappa(F)$ en fonction d'un certain module d'Iwasawa, un résultat en général strictement plus fin que les majorations de Washington et Ozaki (théorème 1 ci-dessous). Enfin, pour un corps de nombres totalement réel, l'étude de la propagation de la nullité de $\kappa(F)$ le long de la tour cyclotomique (sous certaines conditions) est liée aux égalités dites du "miroir" (théorème 4).

Remerciements : l'essentiel de ce travail a été réalisé pendant que le premier auteur était maître de conférences invité à Besançon. Il tient à remercier l'Université de Franche-Comté pour son soutien financier et les membres de l'équipe de Théorie des Nombres de Besançon pour leur hospitalité.

1 Conjecture de Leopoldt et constante de Kummer

On fixe le corps de base F et le nombre premier impair p , et on leur associe les objets suivants :

S : l'ensemble des places au-dessus de p et des places archimédiennes de F ;

$U = U_F$: le groupe des unités de F ;

$\widehat{U} := \widehat{U}_F := U \otimes \mathbb{Z}_p$: le pro- p -complété de U ;

$U' = U'_F$: le groupe des S -unités de F ;
 $\widehat{U}' = \widehat{U}'_F := U' \otimes \mathbb{Z}_p$: le pro- p -complété de U' ;
 L_F (resp L'_F) : la p -extension abélienne non ramifiée (resp. non ramifiée et p -décomposée) maximale de F ;
 A_F (resp A'_F) : la partie p -primaire du groupe de classes (resp S -classes) de F , i.e. $A_F \cong \text{Gal}(L_F/F)$ (resp. $A'_F \cong \text{Gal}(L'_F/F)$) ;
 $M = M_F$: la pro- p -extension abélienne S -ramifiée maximale de F ;
 $\mathcal{X}_F := \text{Gal}(M/F)$;
 $\mathcal{T}_F = \mathcal{T}_F^S$: la \mathbb{Z}_p -torsion de \mathcal{X}_F ;
 \widehat{F} : le composé des \mathbb{Z}_p -extensions de F ;
 F_∞ : la \mathbb{Z}_p -extension cyclotomique de F ;
pour tout $n \geq 0$,
 F_n : le n -ième étage de F_∞/F , $\Gamma_n := \text{Gal}(F_\infty/F_n)$ ($\Gamma = \Gamma_0$), $G_\infty(F_n) := \text{Gal}(F(\mu_{p^\infty})/F_n)$ ($G_\infty := G_\infty(F)$) ;
et pour tout $v \mid p$,
 F_v : le complété de F en la place v ;
 $\widehat{F}_v := \varprojlim F_v^\bullet / F_v^{\bullet p^n}$: le pro- p -complété de F_v^\bullet ;
 U_v : le groupe des unités locales de F_v ;
 $\widehat{U}_v := U_v \otimes \mathbb{Z}_p$: le pro- p -complété de U_v . Comme $v \mid p$, \widehat{U}_v n'est autre que le groupe des unités principales de F_v .
Enfin, pour tout corps L , $\mu_{p^n}(L)$ désignera le groupe des racines p^n -ièmes de l'unité contenues dans L , $\mu(L) := \cup_{n \geq 0} \mu_{p^n}(L)$ et $w(L) = |\mu(L)|$. Si A est un groupe abélien, ${}_n A$ désignera le noyau de la multiplication par n et A/n le conoyau.

La théorie du corps de classes global fournit une description de \mathcal{X}_F au moyen de la suite exacte du corps de classes relative à l'inertie :

$$\widehat{U}_F \xrightarrow{\alpha} \prod_{v \mid p} \widehat{U}_v \xrightarrow{A} \mathcal{X}_F \longrightarrow A_F \longrightarrow 0 \quad (1.1)$$

où α est l'application naturelle "pro- p -diagonale" et A (Artin) envoie chaque facteur \widehat{U}_v sur le groupe d'inertie en v . La conjecture de Leopoldt affirme que l'application α est injective. La version suivante de la conjecture de Leopoldt est bien connue (voir *e.g.* [G], [L], [S], ...)

Proposition 1 *Soit F un corps de nombres et soit p un nombre premier. Les conditions suivantes sont équivalentes :*

- i) la conjecture de Leopoldt est vérifiée pour (F, p)*
- ii) pour tout entier $s \geq 1$, il existe un entier $t \geq 1$ tel que*

$$\forall u \in U \ (u \in U_v^{p^t}, \forall v \mid p) \Rightarrow u \in U^{p^s}$$

- iii) il existe un entier $c \geq 0$ tel que*

$$\forall n \geq 1, \forall u \in U, (u \in U_v^{p^{c+n}}, \forall v \mid p) \Rightarrow u \in U^{p^n}$$

iv) il existe un entier $c \geq 0$ tel que

$$\forall n \gg 0, \forall u \in U, (u \in U_v^{p^{c+n}}, \forall v \mid p) \Rightarrow u \in U^{p^n}$$

Preuve

i) \iff ii) : l'injection naturelle $U \hookrightarrow \prod_{v \mid p} U_v$ induit pour tout $t \geq 1$ un homomorphisme naturel $\alpha_t : U/p^t \rightarrow \prod_{v \mid p} U_v/p^t$, qui donne, par passage à la limite projective, l'application $\alpha : \widehat{U}_F \rightarrow \prod_{v \mid p} \widehat{U}_v$ et l'on a $\ker(\alpha) = \varprojlim \ker(\alpha_t)$. Pour tous entiers $t \geq s \geq 1$, considérons alors le diagramme commutatif :

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker(\alpha_t) & \longrightarrow & U/p^t & \xrightarrow{\alpha_t} & \prod_{v \mid p} U_v/p^t \\ & & a_{s,t} \downarrow & & b_{s,t} \downarrow & & c_{s,t} \downarrow \\ 0 & \longrightarrow & \ker(\alpha_s) & \longrightarrow & U/p^s & \xrightarrow{\alpha_s} & \prod_{v \mid p} U_v/p^s \end{array}$$

où les flèches verticales $a_{s,t}$, $b_{s,t}$ et $c_{s,t}$ sont naturelles. Comme la conjecture de Leopoldt est équivalente à la trivialité de l'homomorphisme $a_{s,t}$ pour $t \gg s$, l'équivalence i) \iff ii) s'ensuit.

ii) \implies iii) (voir [L]) : soit r un entier positif tel que p^r tue la torsion de tous les U_v , $v \mid p$. D'après ii), il existe un entier $c \geq 0$ tel que

$$\forall u \in U, (u \in U_v^{p^{c+1}}, \forall v \mid p) \Rightarrow u \in U^{p^{r+1}} \quad (1.2)$$

On va montrer par récurrence sur n que c vérifie iii) :

le cas $n = 1$ résulte de (1.2). Supposons $n > 1$ et soit u une unité de F telle que $(u \in U_v^{p^{c+n}}, \forall v \mid p)$. D'après (1.2), il existe $\epsilon \in U_F$ tel que $u = \epsilon^{p^{r+1}}$. Ainsi, $u = \epsilon^{p^{r+1}} = (\epsilon^{p^r})^p \in (U_v^{p^{c+n-1}})^p$, pour tout $v \mid p$. Grâce au choix de r , on en déduit que $\epsilon^{p^r} \in U^{p^{n-1}}$, soit $u \in U^{p^n}$. On a bien montré que ii) \implies iii).

Les implications iii) \implies ii), iii) \implies iv) et iv) \implies i) sont évidentes. **Q.E.D.**

Remarque 1 Si F contient μ_p et admet une seule place au-dessus de p , ou F ne contient pas μ_p et aucune place de F divisant p ne se décompose totalement dans $F(\mu_p)$, il suffit de vérifier la propriété iii) pour $n = 1$ (voir e.g. [L] 2.2.5).

Définition 1 La constante minimale $\kappa = \kappa(F)$ pour laquelle la propriété

$$(\mathcal{L}) \quad \exists c = c(F) \geq 0 / \forall n \gg 0, \forall u \in U_F, (u \in F_v^{p^{n+c}}, \forall v \mid p) \Rightarrow u \in U_F^{p^n}$$

est vérifiée sera appelée constante de Kummer du corps F .

Remarque 2 *Washington ([W1], [W2]) et Ozaki ([O]) donnent des majorations d'une constante qui peut être interprétée comme la plus petite constante vérifiant la propriété iii) de la proposition 1. En fait, dans un certain nombre de cas, la constante de Kummer κ est aussi la valeur minimale des constantes vérifiant la condition iii) de la proposition 1 : c'est le cas, par exemple, si F ne contient pas μ_p ou F est le corps cyclotomique $\mathbb{Q}(\mu_{p^n})$ (qui englobent les cas considérés dans [W1], [W2] et [O]). La démonstration est élémentaire, nous n'entrons pas dans les détails.*

Dans le théorème qui suit, qui est le résultat principal de cette section, nous déterminerons la constante de Kummer $\kappa(F)$ comme l'exposant d'un certain module d'Iwasawa. Nous supposons dans la suite de cet article que le corps F vérifie la conjecture de Leopoldt au nombre premier p . Rappelons d'abord la définition du *module de Bertrandias-Payan* ([BP], [N1], [N2], ...) :

Définition 2 *Nous dirons qu'une p -extension (nécessairement cyclique) d'un corps de nombres F est infiniment plongeable si elle est plongeable dans une p -extension cyclique de degré arbitrairement grand.*

Par le corps de classes, une p -extension L/F est infiniment plongeable si et seulement si, pour toute place v de F , l'extension complétée L_v/F_v est plongeable dans une \mathbb{Z}_p -extension de F_v ([BP], [J], [N2], ...). Il en résulte en particulier que L/K est non ramifiée en dehors des places divisant p .

Notons F^{BP} le composé de toutes les p -extensions infiniment plongeables et $T = T_F$ la \mathbb{Z}_p -torsion de $\text{Gal}(F^{BP}/F)$. Alors $\tilde{F} \subset F^{BP} \subset M$ et $T = \text{Gal}(F^{BP}/\tilde{F})$, où \tilde{F} est le composé des \mathbb{Z}_p -extensions de F . Nous avons besoin de quelques notations supplémentaires qui seront utilisées dans la suite de cet article :

Notons comme d'habitude $X_\infty(F)$ (resp. $X'_\infty(F)$) le groupe de Galois sur F_∞ de la pro- p -extension abélienne non ramifiée (resp. non ramifiée et décomposant totalement toutes les places au-dessus de p) maximale de F_∞ , λ_F (resp. λ'_F) l'invariant lambda de $X_\infty(F)$ (resp. $X'_\infty(F)$) (nous supposons que l'invariant mu est nul) et $(X_\infty(F))^0$ (resp. $(X'_\infty(F))^0$) le sous-module fini maximal de $X_\infty(F)$ (resp. $X'_\infty(F)$). Rappelons que $(X_F)^0$ (resp. $(X'_F)^0$) est isomorphe au noyau de la flèche naturelle $j_{n,m} : A_n \rightarrow A_m$ (resp. $A'_n \rightarrow A'_m$), pour $m \gg n \gg 0$, ou encore à celui de $j_n : A_n \rightarrow A_\infty$ (resp. $A'_n \rightarrow A'_\infty$), où $A_n := A_{F_n}$, $A'_n := A'_{F_n}$ et $A_\infty = A_\infty(F) := \varinjlim A_n$ avec les morphismes de liaison $j_{n,m}$ pour $n \leq m$ (voir [I], [K]). Enfin, pour tout module d'Iwasawa Y de Λ -torsion ($\Lambda := \mathbb{Z}_p[[T]]$ est l'algèbre d'Iwasawa), $\alpha(Y)$ (resp. $\beta(Y)$) désignera comme d'habitude l'adjoint (resp. le co-adjoint, c'est-à-dire le dual de l'adjoint) en théorie d'Iwasawa de Y (voir *e.g.* [W3] chap. 15). Rappelons dans une proposition "fourre-tout" les principales propriétés du module de Bertrandias-Payan T_F dont nous aurons besoin dans la suite :

Proposition 2 1) Les modules \mathcal{T}_F^S et T_F sont reliés à l'aide de la suite exacte :

$$0 \longrightarrow \mu(F) \longrightarrow \prod_{v|p} \mu(F_v) \longrightarrow \mathcal{T}_F^S \longrightarrow T_F \longrightarrow 0 \quad (1.3)$$

2) Soit $E = F(\mu_p)$. Alors $T_F \cong \text{Hom}(X'_\infty(E), \mu_{p^\infty})^{G_\infty} \cong \text{Hom}(X'_\infty(E)(-1), \mathbb{Q}_p/\mathbb{Z}_p)^{G_\infty}$.

3) Si $G_n = \text{Gal}(F_n/F)$, alors $T_F \cong (T_{F_n})^{G_n}$.

4) Soit $T_\infty = T_\infty(F) := \varprojlim T_{F_n}$ le module de Bertrandias-Payan de F_∞ . Si F est totalement réel, alors $T_\infty(F)$ vérifie la co-descente galoisienne, i.e. $(T_\infty)_\Gamma \cong T_F$.

Preuve Pour 1) et 2), voir [N1], th. 4.2 et [N2] th 1.2. La propriété 3) est une conséquence immédiate de 2). Reste à montrer 4) (voir aussi [B]). Réécrivons la suite exacte (1.3) sous la forme

$$0 \longrightarrow W_F \longrightarrow \mathcal{T}_F \longrightarrow T_F \longrightarrow 0.$$

Par passage à la limite projective, on obtient une suite exacte de Λ -modules

$$0 \longrightarrow W_\infty(E) \longrightarrow \mathcal{T}_\infty(E) \longrightarrow T_\infty(E) \longrightarrow 0.$$

D'où, par le lemme du serpent (G_∞ est pro-cyclique car $p \neq 2$)

$$\dots \longrightarrow T_\infty(E)^{G_\infty} \longrightarrow W_\infty(E)_{G_\infty} \longrightarrow \mathcal{T}_\infty(E)_{G_\infty} \longrightarrow T_\infty(E)_{G_\infty} \longrightarrow 0.$$

Or $T_\infty(E)^{G_\infty} = \alpha(X'_\infty(E)^{-}(-1))^{G_\infty} = 0$ par Leopoldt (voir [N1]) et $W_\infty(E)_{G_\infty} = W_F$ pratiquement par définition. De plus $\mathcal{T}_\infty(E)_{G_\infty} = \mathcal{T}_\infty(E)_\Gamma$ et si F est totalement réel, $T_\infty(E)_\Gamma = T_F$. **Q.E.D.**

Les suites exactes (1.1) et (1.3) montrent que l'application naturelle $\mathcal{T}_F \longrightarrow A_F$ se factorise à travers une application induite

$$\psi_F : T_F \longrightarrow A_F$$

qui jouera un rôle central dans la suite. Les suites exactes (1.1) et (1.3) montrent aussi que l'image de ψ_F est le groupe de Galois $\text{Gal}(\tilde{F}L_F/\tilde{F})$ et son noyau $\ker(\psi_F)$ est le groupe de Galois $\text{Gal}(F^{BP}/\tilde{F}L_F)$. Nous pouvons maintenant déterminer la constante de Kummer κ pour tout corps de nombres

Théorème 1 Soit F un corps de nombres vérifiant la conjecture de Leopoldt au nombre premier p . Soit $\kappa = \kappa(F)$ sa constante de Kummer. Alors p^κ est l'exposant du module $\text{Gal}(F^{BP}/\tilde{F}L_F) = \ker(\psi_F)$.

Remarque 3 Si F est totalement réel, $\tilde{F} = F_\infty$ et $M \supseteq F^{BP} \supseteq LF_\infty \supseteq F_\infty$. L'exposant de $\text{Gal}(F^{BP}/F_\infty L_F)$ est donc inférieur ou égal à l'exposant p^e de $\text{Gal}(M/F_\infty)$. C'est ce dernier qui intervient dans la preuve du théorème principal d'Ozaki ([O]). Ozaki applique

ensuite directement la Conjecture Principale pour donner une expression analytique de e . Dans le cas particulier des corps cyclotomiques $K_n = \mathbb{Q}(\mu_{p^n})$, K_n admet une seule place au-dessus de p et donc $K_n^{BP} = M_S(K_n)$. La constante déterminée dans le théorème 1 coïncide alors avec celle de Washington ([Wa1], [Wa2]) si la conjecture de Vandiver (affirmant que p ne divise pas le nombre de classes du sous-corps réel maximal de $\mathbb{Q}(\mu_p)$) est vérifiée au nombre premier p (sinon, elle est plus petite que celle de Washington).

Preuve Notons \mathcal{I} (pour inertie) le conoyau de l'homomorphisme α dans la suite exacte du corps de classes (1.1), nous avons deux suites exactes :

$$0 \longrightarrow \widehat{U}_F \xrightarrow{\alpha} \prod_{v|p} \widehat{U}_v \xrightarrow{A} \mathcal{I} \longrightarrow 0 \quad (1.4)$$

$$0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{X}_F \longrightarrow A_F \longrightarrow 0 \quad (1.5)$$

où l'injectivité de α dans la première suite exacte provient du fait que F vérifie la conjecture de Leopoldt au nombre premier p . En appliquant, pour tout entier $n \geq 1$, le lemme du serpent aux deux suites, nous obtenons les suites exactes

$$0 \longrightarrow \mu_{p^n}(F) \longrightarrow \prod_{v|p} \mu_{p^n}(F_v) \xrightarrow{f_n} \mathcal{I} \longrightarrow U/p^n \xrightarrow{\alpha_n} \prod_{v|p} U_v/p^n \quad (1.6)$$

$$0 \longrightarrow {}_p \mathcal{I} \longrightarrow {}_p \mathcal{T}_S \longrightarrow {}_p A_F \longrightarrow \dots \quad (1.7)$$

Comme la \mathbb{Z}_p -torsion de \mathcal{I} est finie (suite exacte (1.7)), les noyaux $\ker(\alpha_n) (\cong \text{coker}(f_n))$ sont bornés (notations de la suite exacte (1.6)). Soit n suffisamment grand pour que p^n tue la torsion \mathcal{T}_F . On a ${}_p \mathcal{I} = t(\mathcal{I}) := \mathbb{Z}_p$ -torsion de \mathcal{I} et le diagramme commutatif

$$\begin{array}{ccccccc} 0 & \longrightarrow & t(\mathcal{I}) & \longrightarrow & \mathcal{T}_F & \longrightarrow & A_F \\ & & f_n \uparrow & & \parallel & & \uparrow \psi_F \\ 0 & \longrightarrow & W := \prod_{v|p} \mu(F_v)/\mu(F) & \longrightarrow & \mathcal{T}_F & \longrightarrow & T_F \longrightarrow 0 \end{array}$$

montre que $\ker(\psi_F) \cong \text{coker}(f_n) \cong \ker(\alpha_n)$. Il reste donc à montrer le

Lemme 1 p^κ est l'exposant de $\ker(\alpha_n)$, pour n assez grand.

Preuve du lemme. Soit p^d l'exposant de $\ker(\alpha_n)$, pour n assez grand. Par définition de κ (voir la condition *iv*) de la proposition 1), p^κ tue le noyau de $\alpha_n : U/p^n \longrightarrow \prod_{v|p} U_v/p^n$, donc $d \leq \kappa$.

Pour montrer l'inégalité inverse, prenons $n \gg 0$ et considérons le diagramme commutatif issu des suites exactes du serpent (1.6)

$$\begin{array}{ccccccc} 0 & \longrightarrow & W & \xrightarrow{f_{n+d}} & t(\mathcal{I}) & \xrightarrow{\pi_{n+d}} & \ker(\alpha_{n+d}) \longrightarrow 0 \\ & & \downarrow p^d & & \downarrow p^d & & \downarrow nat \\ 0 & \longrightarrow & W & \xrightarrow{f_n} & t(\mathcal{I}) & \xrightarrow{\pi_n} & \ker(\alpha_n) \longrightarrow 0 \end{array}$$

Ce diagramme montre que si $u \bmod U^{p^{n+d}} \in \ker(\alpha_{n+d})$, alors $u \bmod U^{p^n}$ est trivial dans $\ker(\alpha_n)$ car $p^d \text{ tue } \text{coker}(f_{n+d}) \cong \ker(\alpha_{n+d})$. Autrement dit, la constante de Kummer κ vérifie la condition *iv*) de la proposition 1, *i.e.* $d \geq \kappa$. **Q.E.D.**

Exemples Soit F un corps de nombres tel que $T_F = 0$. Alors $\kappa_n := \kappa(F_n) = 0$ pour tout étage F_n , $n \geq 0$, de la \mathbb{Z}_p -extension cyclotomique de F . Les exemples standard de tels corps sont les corps de nombres p -rationnels introduits dans [MN] (ce sont les corps pour lesquels \mathcal{T}_F^S est trivial) qui sont une généralisation des corps cyclotomiques $K = \mathbb{Q}(\mu_p)$, p régulier, et qui vérifient donc le lemme de Kummer (voir aussi [MN] corollaire 2)

Comme conséquence du lemme 1, on a

Corollaire 1 *Soit F un corps CM et soit F^+ le sous-corps réel maximal de F . Alors les constantes de Kummer des corps F et F^+ sont égales.*

Preuve Notons $\kappa = \kappa(F)$ et $\kappa^+ = \kappa(F^+)$. Soit n un entier assez grand pour que p^n tue \mathcal{T}_F et $\prod_{v|p} \mu(F_v)$. En particulier, p^κ est l'exposant de $\ker \alpha_n$ (preuve du lemme 1). Comme

p est impair, on a, avec les notations $+$ et $-$ habituelles : $\ker \alpha_n \cong (\ker \alpha_n)^+ \oplus (\ker \alpha_n)^-$.

Mais $(\ker \alpha_n)^- \cong \ker(\alpha_n^- : (U/p^n)^- \longrightarrow (\prod_{v|p} U_v/p^n)^-)$ et l'application α_n^- n'est autre que

l'injection naturelle $\mu(F) \hookrightarrow (\prod_{v|p} \mu(F_v))^-$ (par le choix de n). D'où $(\ker \alpha_n)^- = 0$ (en

notation additive). En conséquence p^κ est l'exposant de $(\ker \alpha_n)^+ = \ker(\alpha_n^+ : (U/p^n)^+ \longrightarrow (\prod_{v|p} U_v/p^n)^+)$. Comme p est impair, $(U/p^n)^+ \cong U_{F^+}/p^n$ et $(\ker \alpha_n)^+$ n'est autre que

le noyau de l'application naturelle $U_{F^+}/p^n \longrightarrow (\prod_{v|p} U_v/p^n)^+$ dont l'exposant est p^{κ^+} .

Q.E.D.

Anecdotiquement, on peut se demander si la réciproque de la formulation initiale du lemme de Kummer est valable :

Corollaire 2 *Soit F un corps de nombres totalement réel tel que $F_\infty \cap L_F = F$. Alors (i) $\kappa(F) = 0$ si et seulement si $T_F = \text{Gal}(F^{BP}/F_\infty) \cong A_F$.*

(ii) Si, en plus, aucune place de F au-dessus de p ne se décompose totalement dans $F(\mu_p)$, alors $\kappa(F) = 0$ si et seulement si $\mathcal{T}_F \cong A_F$.

(iii) Si le corps $F = \mathbb{Q}(\mu_p)^+$ vérifie la conjecture de Vandiver, alors $\kappa(F) = 0$ si et seulement si le nombre premier p est régulier.

Preuve L'hypothèse $F_\infty \cap L_F = F$ signifie que l'application naturelle $\psi_F : T(F) \rightarrow A_F$ est surjective. D'où (i). La condition de non-décomposition signifie que $\mu(F_v) = 1$ pour tout $v \mid p$, et donc que $T_F \cong \mathcal{T}_F$. D'où (ii). Prenons maintenant $F = \mathbb{Q}(\mu_p)^+$. D'après (ii) et la conjecture de Vandiver, $\kappa(F) = 0$ si et seulement si $\mathcal{T}_F = 0$, i.e. le corps F est p -rationnel ([MN]) et l'on sait que cette condition est équivalente à la régularité de p (voir e.g. [MN]). **Q.E.D.**

Grâce au théorème 1 et à la formule analytique de Coates ([C]), nous sommes également en mesure de donner, pour tout corps de nombres totalement réel, la majoration suivante de κ qui généralise et améliore les majorations de Washington ([W1], [W2]) et Ozaki ([O]).

Théorème 2 Si F est un corps de nombres totalement réel vérifiant la conjecture de Leopoldt au nombre premier p , alors :

$$p^\kappa \leq p^{n_0 - f} \cdot \left| \frac{R_p(F)}{\sqrt{|D(F)|}} \right|_p^{-1} \cdot \frac{w(F(\mu_p))}{\prod_{v \mid p} w(F_v)},$$

où $p^{n_0} = |\text{Gal}(L_F \cap F_\infty/F)|$ et pour toute place v divisant p , f_v est l'indice d'inertie absolu en la place v et $f := \sum_{v \mid p} f_v$.

Preuve Nous avons $p^\kappa \leq |\ker(\psi_F)|$, où ψ_F est l'application naturelle de T_F dans A_F définie par le corps de classes (preuve du théorème précédent). Il est clair que l'ordre de l'image de ψ_F est égal à h_F/p^{n_0} , où h_F est l'ordre de A_F . L'ordre du module de Bertrandias-Payan T_F s'exprime aisément en fonction de celui de \mathcal{T}_F grâce à la suite exacte (1.3) :

$$|T_F| = |\mathcal{T}_F| \cdot w(F) / \left(\prod_{v \mid p} w(F_v) \right)$$

Il est bien connu, par ailleurs, que

$$|\mathcal{T}_F| \sim w(F(\mu_p)) \cdot h_F \cdot \prod_{v \mid p} (1 - (Nv)^{-1}) \cdot R_p(F) / \sqrt{|D(F)|}$$

(voir [C] app.). Comme $N(v) = p^{f_v}$ et $|\mu(F)| = 1$, nous en déduisons $|\ker(\psi_F)|$ et donc la majoration escomptée de p^κ . **Q.E.D.**

Corollaire 3 (généralise [A] Theorem 6.5) Avec les hypothèses et notations du théorème précédent, $\kappa(F) = 0$ si et seulement si

$$R_p(F)/\sqrt{|D(F)|} \sim p^{f-n_0} \left(\prod_{v|p} w(F_v) \right) (w(F(\mu_p))^{-1},$$

où le signe \sim désigne l'égalité à une unité p -adique près.

Preuve On a $\kappa(F) = 0$ si et seulement si $\ker(\psi_F)$ est nul. Or l'ordre de ce module a été calculé dans la preuve du théorème précédent. **Q.E.D.**

2 Propagation dans la tour cyclotomique de la nullité de la constante de Kummer

Dans ce paragraphe, nous donnons des critères de montée pour la nullité de la constante de Kummer dans la tour cyclotomique d'un corps de nombres F (totalement réel). Nous avons besoin de deux lemmes.

Lemme 2 Soit F un corps de nombres quelconque et soit n un entier ≥ 0 . Si $(A_\infty)^{\Gamma_n}$ est fini alors :

$$|(A_\infty)^{\Gamma_n}| = \frac{|(X_\infty)_{\Gamma_n}|}{|(X_\infty)^{\Gamma_n}|}. \text{ En particulier, si } (X_\infty)^0 = 0, |(A_\infty)^{\Gamma_n}| = |(X_\infty)_{\Gamma_n}|.$$

Preuve du lemme On peut supposer $n = 0$. D'après la théorie de l'adjoint ([I] ou [W3] chap. 13), $A_\infty \simeq \beta(Y_\infty)$ où Y_∞ est un sous-module d'indice fini de X_∞ . En particulier, X_∞ et Y_∞ ont la même série caractéristique $f(T)$. Il vient :

$$|(A_\infty)^\Gamma| = |\beta(Y_\infty)^\Gamma| = |\alpha(Y_\infty)_\Gamma| \sim f(0) \text{ (car } \alpha(Y_\infty)^\Gamma = 0 \text{ comme sous-module fini d'un adjoint) et } f(0) \sim \frac{|(X_\infty)_\Gamma|}{|(X_\infty)^\Gamma|}. \text{ Q.E.D.}$$

À partir de maintenant, on suppose (sauf mention du contraire) que F est totalement réel et que tous les étages de la tour cyclotomique de F vérifient la conjecture de Leopoldt en p . Les constantes de Kummer $\kappa_n = \kappa(F_n)$ existent et l'on se propose d'étudier leur nullité asymptotique. Pour plus de clarté, mettons ici en exergue quelques conséquences de la conjecture de Leopoldt pour les corps totalement réels (voir [Gr]) :

- i) $A_\infty(F) \xrightarrow{\sim} A'_\infty(F)$ ou de façon équivalente, le noyau de $X_\infty(F) \twoheadrightarrow X'_\infty(F)$ est fini. Il en résulte en particulier que $\lambda = \lambda'$ pour F_∞/F .
- ii) $A_\infty(F)^\Gamma$ est fini ou, de façon équivalente, $X_\infty(F)^\Gamma$ (resp. $X_\infty(F)_\Gamma$) est fini. En particulier, le lemme 2 s'applique.

Dans toute la suite, pour F fixé et pour tout entier $n \geq 1$, on notera $\kappa_n := \kappa(F_n)$, $A_n := A_{F_n}$ et $T_n := T_{F_n}$.

Lemme 3 *Supposons*

$$(*) \quad L_F \cap F_\infty = F.$$

Alors, pour $n \geq 0$ fixé, les conditions suivantes sont équivalentes :

- i) $\kappa_n = 0$;*
- ii) $\kappa(F) = 0$ et l'application naturelle $j_{0,n} : A_F \longrightarrow (A_n)^{G_n}$ est injective;*
- ii') $\kappa(F) = 0$ et $j_{0,n}$ est un isomorphisme;*
- iii) $\kappa_m = 0$ pour tout entier m tel que $0 \leq m \leq n$.*

Preuve Dans le carré commutatif :

$$\begin{array}{ccc} (T_n)^{G_n} & \xrightarrow{\psi_n} & (A_n)^{G_n} \\ \uparrow & & \uparrow j_{0,n} \\ T_F & \xrightarrow{\psi_F} & A_F \end{array}$$

la flèche verticale de gauche est l'homomorphisme dual de l'application naturelle $X'(-1)_{G_\infty(F_n)} \longrightarrow X'(-1)_{G_\infty(F)}$ et est un isomorphisme à cause de l'expression du module de Bertrandias-Payan comme module de descente (proposition 2 iii)). L'injectivité de ψ_n (c'est-à-dire la nullité de κ_n) est donc équivalente à celles de ψ_F et $j_{0,n}$. D'où l'équivalence $i) \iff ii)$. Pour $ii) \iff ii')$, il suffit de remarquer que si la propriété $ii)$ est vérifiée alors ψ et ψ_n sont des isomorphismes à cause de $(*)$. Pour $ii) \iff iii)$, $j_{0,n}$ est injective si et seulement si $j_{0,m}$ est injective pour tout m , $0 \leq m \leq n$. **Q.E.D.**

Remarque 4 *Le carré commutatif ci-dessus (preuve du lemme 3) montre aussi que si $\kappa_n = 0$ alors $\kappa_m = 0$ pour tout entier m , $0 \leq m \leq n$, indépendamment de l'hypothèse $(*)$ (i.e. de la surjectivité de ψ_F).*

Dans toute la suite, pour F fixé, on notera N_1 le plus petit entier tel que F_{N_1} vérifie l'hypothèse $(*)$ du lemme précédent, et N_2 le plus petit entier tel que $\ker(j_{N_2})$ soit isomorphe à $(X_\infty^0)^{\Gamma_{N_2}} \cong (X_\infty)^{\Gamma_{N_2}}$. L'existence de N_1 provient de considérations élémentaires de ramification, et celle de N_2 de considérations sur la capitulation (voir e.g. [I] ou [K]). On pose $N = \sup(N_1, N_2)$.

Théorème 3 *Avec les hypothèses et notations précédentes, les conditions suivantes sont équivalentes :*

- i) $\kappa_n = 0$ pour n assez grand ;*
- ii) $\kappa_N = 0$ et l'application naturelle $j_N : A_F \longrightarrow (A_\infty)^\Gamma$ est injective (donc est un isomorphisme) ;*
- iii) $\kappa_N = 0$ et $(X_\infty)^0 = 0$;*
- iv) $(X_\infty)^0 = 0$ et $T_N \xrightarrow{\sim} A_N$ (donc $T_N \xrightarrow{\sim} (X_\infty)_{\Gamma_N} \xrightarrow{\sim} A_N$).*

Remarque 5 Dans ces énoncés, on peut remplacer N par un entier n supérieur ou égal à N .

Preuve $i) \iff ii)$ d'après le lemme 3.

$ii) \iff iii)$ par le choix de N , en remarquant que $(X_\infty)^0 = 0 \iff ((X_\infty)^0)^{\Gamma_N} = 0$.

$iii) \implies iv)$: par le choix de N et parce que F_N est totalement réel, $\kappa_N = 0$ si et seulement si $T_N \xrightarrow{\sim} A_N$ (preuve du lemme précédent). De plus comme F est totalement réel, $T_N \twoheadrightarrow X_\infty$ et, par co-descente, on a $(T_\infty)_{\Gamma_N} \cong T_N \twoheadrightarrow (X_\infty)_{\Gamma_N} \twoheadrightarrow A_N$ (proposition 2 $iv)$). Les isomorphismes annoncés dans $iv)$ en résultent.

$iv) \implies iii)$: c'est évident. **Q.E.D.**

Corollaire 4 Supposons que F admet une seule place au-dessus de p , totalement ramifiée dans la tour cyclotomique de F ; alors $\kappa_n = 0$ pour tout $n \geq 0$ si et seulement si $\kappa(F) = 0$ et $(X_\infty(F))^\Gamma = 0$.

Preuve Les conditions de ramification imposées entraînent que $(X_\infty(F))_{\Gamma_n} \xrightarrow{\sim} A_n$ pour tout $n \geq 0$, donc $N = 0$ dans le théorème précédent. **Q.E.D.**

Remarque 6 Dans le lemme 3 et le théorème 3, la surjectivité de $\Psi_N : T_N \twoheadrightarrow A_N$ joue un rôle-clé. On peut se demander ce qui subsiste si l'on enlève l'hypothèse que F est totalement réel :

$i)$ On peut ajouter l'hypothèse que $(X_\infty(F))^0 = 0$ (qui est restrictive ; voir e.g. [Gr]). Les arguments du lemme 3 montrent alors que la nullité de $\kappa(F)$ se propage dans la tour cyclotomique de F .

$ii)$ Pour les corps CM , on peut toujours se ramener au sous-corps réel maximal (d'après le corollaire 1). Noter que la propriété $iv)$ du théorème précédent n'est pas forcément vérifiée pour un corps CM (voir aussi la fin de la section 4).

Si F est un corps de nombres quelconque, on peut donner la caractérisation suivante de la nullité des constantes de Kummer dans la tour cyclotomique de F . Nous avons besoin d'une notation supplémentaire. Soit

$$\Psi : \text{Hom}(X'_\infty(E), \mu_{p^\infty})^\Delta \longrightarrow A_\infty(F)$$

($E = F(\mu_p)$ et $\Delta := \text{Gal}(E/F)$) l'homomorphisme obtenu par passage à la limite inductive sur les

$$\psi_n : \text{Hom}(X'_\infty(E), \mu_{p^\infty})^{G_\infty(F_n)} \longrightarrow A_n$$

avec des morphismes de liaison naturels (voir preuve du lemme 3). Comme $\ker(\psi_n) \hookrightarrow \ker(\psi_m)$ pour $n \leq m$, le résultat suivant est alors évident

Proposition 3 *Soit F un corps de nombres quelconque. Alors $\kappa_n = 0$ pour tout $n \geq 0$ si et seulement si l'homomorphisme naturel*

$$\Psi : \text{Hom}(X'_\infty(E), \mu_{p^\infty})^\Delta \longrightarrow A_\infty(F)$$

est injectif

3 Corps CM et invariants d'Iwasawa

Dans toute cette section, on suppose que F est un corps de nombres totalement réel et que tous les étages F_n de la tour cyclotomique de F vérifient la conjecture de Leopoldt. Soient $E = F(\mu_p)$ et $\Delta = \text{Gal}(E/F)$. On suppose que Δ est d'ordre 2 (*i.e.* F est le sous-corps réel maximal de E). Ce n'est pas une restriction : pour tout sous-corps totalement réel de E , il suffit de faire intervenir le caractère pair correspondant χ et le caractère miroir $\chi^* = \chi^{-1}\omega$, où ω est le caractère de Teichmüller; cela n'apporte pas grand chose à part des complications d'écriture.

Puisque p est impair, tout module d'Iwasawa Y attaché au corps $E = F(\mu_p)$ se décompose de façon canonique sous la forme $Y = Y^+ \oplus Y^-$ pour l'action de Δ . Soient λ^+ , λ^- , λ'^+ et λ'^- les invariants lambda attachés respectivement à $X_\infty(E)^+$, $X_\infty(E)^-$, $X'_\infty(E)^+$ et $X'_\infty(E)^-$ (on supposera que l'invariant mu est nul). Avant de donner le résultat principal de cette section, il convient de faire quelques rappels sur "le miroir" qui permet de comparer les invariants "plus" et "moins" attachés aux différents modules d'Iwasawa. La proposition ci-dessous sera une conséquence immédiate de la surjectivité de l'homomorphisme $\psi_\infty : T_\infty(F) \longrightarrow X_\infty(F)$ et du fait que $T_\infty \cong \varprojlim \text{Hom}(X'_\infty(E), \mu_{p^\infty})^{G_\infty(F_n)} \cong \alpha(X'_\infty(E)^-(-1))$. Comme dans le paragraphe précédent, on adopte les notations : $T_n := T_{F_n}$, $A_n := A_{F_n}$ et $\kappa_n := \kappa(F_n)$.

Proposition 4 *Soit F un corps totalement réel tel que F soit le sous-corps réel maximal de $E = F(\mu_p)$. On suppose que l'invariant μ de $X_\infty(E)$ est nul. Alors :*

1) $\lambda'^- \geq \lambda^+ + \dim_{\mathbb{F}_p}(X_F)^0/p$. En particulier, si $\lambda'^- = \lambda^+$ alors $(X_\infty(F))^0 = 0$.

2) *Les conditions suivantes sont équivalentes :*

i) $\lambda'^- = \lambda^+$;

ii) *l'homomorphisme naturel $\psi_\infty : T_\infty(F) \rightarrow X_\infty(F)$ est un isomorphisme ;*

iii) *l'homomorphisme naturel $\psi_n : T_n \rightarrow X_\infty(F)_{\Gamma_n}$ est un isomorphisme pour n assez grand ;*

iv) *l'homomorphisme naturel $\psi_n : T_n \rightarrow X_\infty(F)_{\Gamma_n}$ est un isomorphisme pour tout entier $n \geq 0$;*

v) $\psi_F : T_F \xrightarrow{\sim} X_\infty(F)_\Gamma$ et $(X_\infty(F))^0 = 0$.

Remarque 7 *On rappelle que $\lambda^+ = \lambda'^+$, mais on écrit λ^+ dans cette section pour*

souligner le fait qu'on travaille avec le groupe des classes, et non le groupe des S -classes. On utilisera la notation λ'^+ dans la section 4.

Preuve (voir aussi [B]) Comme $\mu = 0$, la première assertion et l'équivalence entre i) et ii) découlent directement de la surjectivité de l'homomorphisme ψ_∞ et du fait que $T_\infty(F)$ ne contient pas de sous-module fini non nul, car c'est un adjoint (voir [N1], [N2]). Les équivalences $ii) \iff iii) \iff iv)$ sont évidentes, de même que l'implication $ii) \implies v)$. $v) \implies ii)$: comme Γ est pro-cyclique, le lemme du serpent appliqué à la suite exacte tautologique $0 \longrightarrow \ker \psi_\infty \longrightarrow T_\infty(F) \longrightarrow X_\infty(F) \longrightarrow 0$ donne par co-descente :

$$X_\infty(F)^\Gamma \longrightarrow (\ker \psi_\infty)_\Gamma \longrightarrow T_\infty(F)_\Gamma \longrightarrow X_\infty(F)_\Gamma \longrightarrow 0$$

Mais $X_\infty(F)^\Gamma = (X_\infty^0)^\Gamma = 0$ et $T_\infty(F)_\Gamma = T_F$ (proposition 2 iv)). $v)$ entraîne alors la nullité de $\ker \psi_\infty$. **Q.E.D.**

Théorème 4 Soit F un corps totalement réel tel que F soit le sous-corps réel maximal de $E := F(\mu_p)$. Soit N l'entier défini dans le théorème 3. Les conditions suivantes sont équivalentes :

- $i)$ $\kappa_n = 0$ pour tout entier $n \gg 0$;
- $ii)$ $\lambda'^- = \lambda^+$ et $(X_\infty(F))_{\Gamma_N} \xrightarrow{\sim} A_N$;
- $iii)$ $\lambda'^- = \lambda^+$ et $(X_\infty(F))_{\Gamma_n} \xrightarrow{\sim} A_n$ pour n assez grand ;
- $iv)$ $\lambda'^- = \lambda^+$ et les invariants ν des systèmes $(X_\infty(F)_{\Gamma_n})$ et (A_n) coïncident ;
- $v)$ $\lambda'^- = \lambda^+$ et l'application naturelle $A_N \longrightarrow A_\infty^{\Gamma_N}$ est surjective (donc est un isomorphisme) ;
- $vi)$ $\lambda'^- = \lambda^+$ et l'application naturelle $A_n \longrightarrow A_\infty^{\Gamma_n}$ est surjective (donc est un isomorphisme), pour $n \gg 0$.

Notons que ces conditions entraînent toutes que $(X_\infty(F))^0 = 0$.

Preuve $i) \iff ii)$ d'après la proposition 4 et le théorème 3, $iv)$.

$ii) \iff iii)$ d'après la remarque 5 et le théorème 3.

$ii) \iff iv)$: d'après les formules asymptotiques donnant l'ordre des groupes $X_\infty(F)_{\Gamma_n}$ et A_n (voir e.g. [W3] chap.13), les invariants λ et μ de ces deux groupes sont les mêmes, mais les invariants ν peuvent *a priori* être différents. Comme $X_\infty(F)_{\Gamma_n} \twoheadrightarrow A_n$ pour $n \gg 0$, l'égalité des invariants ν équivaut à $X_\infty(F)_{\Gamma_n} \xrightarrow{\sim} A_n$. L'équivalence $ii) \iff iv)$ est alors claire.

$ii) \iff v)$: on a déjà fait remarquer que l'égalité $\lambda'^- = \lambda^+$ implique $(X_\infty(F))^0 = 0$. Sous cette dernière condition, la formule du lemme 2 s'écrit $|X_\infty(F)_{\Gamma_N}| = |A_\infty^{\Gamma_N}|$. Or, par le choix de N , $X_\infty(F)_{\Gamma_N} \twoheadrightarrow A_N \hookrightarrow A_\infty^{\Gamma_N}$. L'équivalence cherchée s'en déduit facilement. L'équivalence $ii) \iff vi)$ se démontre de la même façon. **Q.E.D.**

Remarque 8 Le conoyau de $j_n : A_n \longrightarrow A_\infty^{\Gamma_n}$ a été étudié par plusieurs auteurs (voir les références de [LMN]). Dans le cas totalement réel, la conjecture de Greenberg entraîne

la nullité de $\text{coker}(j_n)$. Cette nullité est automatique si F_n admet une seule p -place, totalement ramifiée dans F_∞ .

Une généralisation raisonnable de la conjecture de Vandiver à un corps de nombres totalement réel est la conjecture de Greenberg qui prédit la nullité de λ_F . Le corollaire 2 se généralise ainsi :

Corollaire 5 *Supposons en plus que F vérifie la conjecture de Greenberg sur la nullité de $\lambda_{E^+} = \lambda_F$. Alors $\kappa_n = 0$ pour tout entier $n \geq 0$ si et seulement si $X'_\infty{}^- = 0$ ($\iff A'_{E_n}^- = 0$ pour $n \gg 0$).*

Si F_∞ admet une seule place au-dessus de p , alors $X_\infty(F)_{\Gamma_n} \xrightarrow{\sim} A_n$ pour tout $n \geq 0$. D'où

Corollaire 6 *Supposons que F admet une seule place au-dessus de p , qui est totalement ramifiée dans F_∞/F . Alors $\kappa_n = 0$ pour tout entier $n \geq 0$ si et seulement si $\lambda'^- = \lambda^+$.*

Dans le cas particulier du corps cyclotomique $E = \mathbb{Q}(\mu_p)$, $A'_{E_n} = A_{E_n}$ pour tout entier $n \geq 0$. En particulier, $\lambda^- = \lambda'^-$. D'où

Corollaire 7 *Si F est le sous-corps réel maximal du corps cyclotomique $\mathbb{Q}(\mu_p)$, alors $\kappa_n = 0$ pour tout entier $n \geq 0$ si et seulement si $\lambda^- = \lambda^+$*

Concernant l'égalité du miroir sans hypothèse supplémentaire, on a le critère suivant :

Théorème 5 *1) $\lambda'^- = \lambda^+$ si et seulement si les constantes κ_n sont bornées.
2) $\lambda^- = \lambda^+$ si et seulement si les constantes κ_n sont bornées et aucune place de F au-dessus de p ne se décompose totalement dans $F(\mu_p)$.*

Preuve 1) Si F est un corps de nombres totalement réel, l'homomorphisme

$$\psi_n : T_n \cong \text{Hom}(X'_\infty(E), \mu_{p^\infty})^{G_\infty(F_n)} \longrightarrow A_n$$

est surjectif pour n assez grand. Rappelons que Ψ est l'homomorphisme obtenu par passage à la limite inductive :

$$\Psi : \text{Hom}(X'_\infty(E), \mu_{p^\infty})^\Delta \longrightarrow A_\infty$$

Comme $\mu = 0$, il est clair que $\lambda'^- = \lambda^+$ si et seulement si $\ker(\Psi)$ est fini. De plus, $\ker(\Psi) = \varinjlim \ker(\psi_n)$ et les morphismes de liaison $\ker(\psi_n) \rightarrow \ker(\psi_m)$ sont injectifs pour $m \geq n \geq 0$. La finitude de $\ker(\Psi)$ est donc équivalente au fait que les constantes κ_n sont bornées.

2) Il est bien connu que $\lambda'^- \geq \lambda^+$ (proposition 4) et $\lambda^- = \lambda'^- + s$, où s est le nombre de places de F au dessus de p qui se décomposent dans $F(\mu_p)$ (voir *e.g.* [I]). Donc, $\lambda^- = \lambda^+$ si et seulement si $\lambda^- = \lambda'^- = \lambda^+$ et 2) découle alors de 1). **Q.E.D.**

Remarque 9 *Si F vérifie la conjecture de Greenberg, combinant le corollaire 5 et le théorème 5, on voit que : $\lambda^- = \lambda^+ \iff X_\infty'^- = 0$ et $s = 0 \iff T_F = 0$ et $s = 0$ (proposition 2, 2)) $\iff \mathcal{T}_F = 0$ (suite exacte (1.3)); i.e. le corps F est p -rationnel ([MN]).*

4 Constante de Kummer pour les S -unités

Dans cette section, nous indiquerons brièvement comment les résultats des paragraphes précédents peuvent s'adapter au groupe des S -unités. Rappelons que S est l'ensemble des places divisant p et des places archimédiennes de F . Si F est un corps de nombres quelconque, la suite exacte du corps de classes relative à la décomposition s'écrit :

$$\widehat{U}'_F \xrightarrow{\alpha} \prod_{v|p} \widehat{F}'_v \xrightarrow{\psi} \mathcal{X}'_F \longrightarrow A'_F \longrightarrow 0 \quad (4.8)$$

où α est l'application naturelle "pro- p -diagonale" et ψ est le produit des homomorphismes de réciprocité locaux envoyant chaque facteur \widehat{F}'_v sur le groupe de décomposition en v . La conjecture de Leopoldt affirme que l'application α est injective. Ainsi, comme pour les unités, il existe une constante minimale $\kappa' = \kappa'(F) \geq 0$ vérifiant la propriété

$$(\mathcal{L}') \quad \forall n \gg 0, \forall u \in U', (u \in F_v^{p^{\kappa'+n}}, \forall v | p) \Rightarrow u \in U'^{p^n}$$

et tous les résultats des paragraphes précédents (hormis le corollaire 1 et les formules analytiques, c'est-à-dire le théorème 2 et le corollaire 4) restent vrais en remplaçant respectivement $\kappa(F)$, L_F , A_F , $X_\infty(F)$, ... par $\kappa'(F)$, L'_F , A'_F , $X'_\infty(F)$, ... En particulier, $p^{\kappa'(F)}$ est l'exposant du module $\text{Gal}(F^{BP}/\widetilde{F}L'_F)$, pour tout corps de nombres F . Comme $L'_F \subset L_F$, il est alors clair que $\kappa(F) \leq \kappa'(F)$ mais les deux constantes ne sont pas *a priori* égales. Rappelons que pour un corps de nombres totalement réel vérifiant la conjecture de Leopoldt, $A'_\infty \cong A_\infty$. Nous adoptons, comme dans les paragraphes précédents, pour F fixé et tout entier $n \geq 1$, les notations : $A'_n = A'_{F_n}$, $T_n := T_{F_n}$ et $\kappa'_n := \kappa'(F_n)$. D'après la proposition 5 (resp. le théorème 5) et son analogue pour les S -unités, nous avons alors le résultat suivant

Proposition 5 Soit F un corps de nombres totalement réel tel que tous les étages de la \mathbb{Z}_p -extension cyclotomique de F vérifient la conjecture de Leopoldt. Alors

- 1) $\kappa_n = 0$ pour tout $n \geq 0$ si et seulement si $\kappa'_n = 0$ pour tout $n \geq 0$.
- 2) Les constantes κ_n sont bornées si et seulement si les constantes κ'_n le sont.

Mais l'intérêt véritable de travailler avec les S -unités est que l'on sera en mesure d'améliorer le théorème 3 qui sera vérifié, en plus du cas totalement réel, pour les corps contenant μ_p . Plus précisément :

Théorème 6 Soit F un corps de nombres tel que tous les F_n vérifient la conjecture de Leopoldt. On définit l'entier N comme dans le théorème 3. On suppose que F est totalement réel ou contient μ_p . Alors les propriétés suivantes sont équivalentes :

- i) $\kappa'_n = 0$ pour tout entier $n \gg 0$;
- ii) $\kappa'_N = 0$ et l'application naturelle $j_N : A'_F \longrightarrow (A'_\infty)^{\Gamma_N}$ est un isomorphisme ;
- iii) $\kappa'_N = 0$, $(X'_\infty)^0 = 0$;
- iv) $(X'_\infty)^0 = 0$ et $T_N \xrightarrow{\sim} A'_N$ (donc $T_N \xrightarrow{\sim} (X'_\infty)_{\Gamma_N} \xrightarrow{\sim} A_N$).

Preuve La démonstration du théorème 3 reposait sur deux points-clés : le lemme 3 et la surjection $\psi_N : T_N \rightarrow A_N$ (qui intervient aussi dans le lemme 3). On peut les remplacer par les lemmes suivants :

Lemme 4 Soit F un corps de nombres contenant μ_p et tel que $L'_F \cap F_\infty = F$; alors pour tout entier $n \geq 1$, $| {}_p T_n | \geq | {}_p A'_n |$

Preuve D'après la proposition 2,

$$T_n \cong \text{Hom}(X'_\infty(F), \mu_{p^\infty})^{\Gamma_n} = \text{Hom}(X'_\infty(F)(-1)/\omega_n, \mathbb{Q}_p/\mathbb{Z}_p)$$

où, comme d'habitude, ω_n désigne l'élément de l'algèbre d'Iwasawa $(1+T)^{p^n} - 1$. Il vient,

$${}_p T_n \cong \text{Hom}(X'_\infty(F)(-1)/(\omega_n, p^n), \mathbb{Q}_p/\mathbb{Z}_p) \cong \text{Hom}((X'_\infty(F)/(p^n, \omega_n))(-1), \mathbb{Q}_p/\mathbb{Z}_p)$$

Par suite $| {}_p T_n | = | X'_\infty(F)/(p^n, \omega_n) | \geq | A'_n/p^n | = | {}_p A'_n |$ à cause de la surjection $(X'_\infty(F))_{\Gamma_n} \rightarrow A'_n$. **Q.E.D.**

Lemme 5 Supposons que $L'_F \cap F_\infty = F$. les propriétés suivantes sont équivalentes :

- i) $\kappa'_n = 0$ pour $n \gg 0$;
- ii) $\kappa'(F) = 0$ et l'application naturelle $j_0 : A'_F \longrightarrow (A'_\infty)^\Gamma$ est injective ;
- ii') $\kappa'(F) = 0$ et j_0 est un isomorphisme.

Preuve Puisque la démonstration dans le cas totalement réel est analogue à celle du lemme 3, on va supposer que F contient μ_p . Le point de départ est, comme dans le lemme 3, le carré commutatif :

$$\begin{array}{ccc} ({}_pT_n)^{G_n} & \xrightarrow{\psi_n^{(p)}} & ({}_pA'_n)^{G_n} \\ \uparrow & & \uparrow j_{0,n}^{(p)} \\ {}_pT_F & \xrightarrow{\psi^{(p)}} & {}_pA'_F \end{array}$$

où l'isomorphisme vertical de gauche résulte de la proposition 2. Le lemme 4 montre que $\psi^{(p)}$ est injectif si et seulement si c'est un isomorphisme. On en déduit que $\psi_n^{(p)}$ (*a fortiori* ψ_n) est injectif si et seulement si $\psi^{(p)}$ et $j_{0,n}^{(p)}$ (*a fortiori* ψ_n et $j_{0,n}$) sont injectifs. D'où $i) \iff ii)$. Supposons que c'est le cas et choisissons n assez grand pour que p^n tue T_F et A'_F . Par ce choix de n , $T_F \xrightarrow{\sim} (T_n)^{G_n} \cong ({}_{p^n}T_n)^{G_n}$ (proposition 2). Le lemme 4 montre que l'homomorphisme injectif $\psi_n^{(p^n)} : {}_{p^n}T_n \longrightarrow {}_{p^n}A'_n$ est en fait un isomorphisme. Le carré commutatif :

$$\begin{array}{ccc} ({}_{p^n}T_n)^{G_n} & \xrightarrow{\psi_n} & ({}_{p^n}A'_n)^{G_n} \\ \uparrow & & \uparrow j_{0,n} \\ T_F & \xrightarrow{\psi} & A'_F \end{array}$$

montre alors que ψ est un isomorphisme et donc que l'application $j_{0,n}$ est un isomorphisme. D'où $ii) \implies ii')$. L'implication inverse est évidente. **Q.E.D.**

L'équivalence entre les conditions $i)$, $ii)$, $iii)$ et $iv)$ du théorème 6 découle immédiatement du lemme 5 et du choix de N . **Q.E.D.**

Références

- [A] **B. Anglès**: Units and norm residue symbol, *Acta Arithmetica* *XCVIII*.1, 33-51 (2001).
- [B] **R. Badino**: Sur les égalités du miroir, *Thèse, Université de Franche-Comté* (2003).
- [BP] **F. Bertrandias et J.-J. Payan**: Γ -extensions et invariants cyclotomiques, *Ann. Sci. École Norm. Sup.* (4) 517-543 (1972).
- [C] **J. Coates**: p -adic L -functions and Iwasawa's theory, dans "Algebraic number fields" *Proc. Sympos. Durham, Academic Press* (1977).
- [G] **G. Gras**: Remarques sur la conjecture de Leopoldt, *C. R. Acad. Sc.* (A) 247, 377-380 (1972).

- [Gr] **R. Greenberg**: On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* 98, 20, 263-284 (1976).
- [I] **K. Iwasawa**: On \mathbb{Z}_l -extensions of algebraic number fields, *Ann. Math.* 98, 246-328 (1973).
- [J] **J.-F. Jaulent**: Dualité dans les corps surcirculaires, Séminaire de Théorie des Nombres, Paris, 1986-1987, *Progress in Math.* 75, *Birkhäuser*, 183-220 (1988).
- [K] **L.V. Kuz'min**: The Tate module of algebraic number fields, *Izv. Akad. Nauk. USSR Ser. Mat.* 36, 267-327 (1972).
- [L] **F. Lorenz**: Some remarks on Leopoldt's conjecture, *Algebra i Analiz* 10-6 (1998) 144-155; translation in *St. Petersburg Math. J.* 10-6, 1005-1013 (1999).
- [LMN] **M. Le Floc'h, A. Movahhedi et T. Nguyen Quang Do**: On capitulation cokernels in Iwasawa theory, *prépublication* (2003).
- [MN] **A. Movahhedi et T. Nguyen Quang Do**: Sur l'arithmétique des corps de nombres p -rationnels, Séminaire de Théorie des Nombres, Paris, 1988-1989, *Birkhäuser*, 155-200 (1990).
- [N1] **T. Nguyen Quang Do**: Sur la \mathbb{Z}_p -torsion de certains modules galoisiens, *Ann. Inst. Fourier* 36-2, 27-46 (1986).
- [N2] **T. Nguyen Quang Do**: Sur la torsion de certains modules galoisiens II, Séminaire de Théorie des Nombres, Paris, 1986-1987, *Progress in Math.* 75, *Birkhäuser*, 271-297 (1988).
- [O] **M. Ozaki**: Kummer's lemma for \mathbb{Z}_p -extensions over totally real number fields, *Acta Arithmetica*, LXXXI.1, 37-43 (1997).
- [S] **J. Sands**: Kummer's and Iwasawa's version of Leopoldt's conjecture, *Canad. Math. Bull.* 31.1, 338-346 (1988)
- [W1] **L. Washington**: Units of irregular cyclotomic fields, *Ill. J. Math.* 23, 635-647 (1979).
- [W2] **L. Washington**: Kummer's lemma for prime power cyclotomic fields, *J. Number Theory* 40, 165-173 (1992).
- [W3] **L. Washington**: Introduction to Cyclotomic Fields, *Springer*, 2nd edition (1997).

Université Moulay Ismail
 Département de Mathématiques et Informatique
 B.P 4010 Beni M'hamed, Meknès (Maroc).
 assim@fsmek.ac.ma

Université de Franche-Comté, UMR 6623
 16, route de Gray
 25030 Besançon cedex (France)
 nguyen@math.univ-fcomte.fr