Mémoire de synthèse des résultats de recherche
pour
l'habilitation à diriger les recherches.

Théorie d'Iwasawa Cyclotomique.

Jean-Robert Belliard

Table des matières

Chapitre 1

Introduction.

1.1 Liste des publications.

1.1.1 Articles parus.

1. *Sur la structure galoisienne des unités circulaires dans les $\mathbb{Z}_p$-extensions*, J. Number Theory **69** (1998), no. 1, 16–49.
2. avec T. Nguyễn-Quang-Dỗ, *Formules de classes pour les corps abéliens réels*, Ann. Inst. Fourier (Grenoble) **51** (2001), no. 4, 903–937.
3. avec H. Oukhaba, *Sur la torsion de la distribution ordinaire universelle attachée à un corps de nombres*, Manuscripta Math. **106** (2001), no. 1, 117–130.
4. *Sous-modules d'unités en théorie d'Iwasawa*, Théorie des nombres, Années 1998/2001, Publ. Math. UFR Sci. Tech. Besançon, 2002, 12 p.
5. avec T. Nguyễn-Quang-Dỗ, *On modified circular units and annihilation of real classes*, Nagoya Math. J. **177** (2005), 77–115.

1.1.2 Prépublications.

1. *Sur la structure galoisienne des unités circulaires dans les $\mathbb{Z}_p$-extensions*, Thèse de l'université Bordeaux I (1997).
2. *Global units modulo circular units : descent without Iwasawa's Main Conjecture*, preprint (2005).
3. Appendice à l'article de M. Lescop, A. Movahhedi et T. Nguyễn-Quang-Dỗ, *Iwasawa descent and co-descent for units modulo circular units*, preprint (2005).

1.2 Introduction.

Je présente dans ce mémoire un aperçu rapide et sans démonstration de la théorie d'Iwasawa cyclotomique. A part de brèves allusions les chapitres 2 et 3 ne parlent pas de mes résultats. Je redonne simplement et sans aucune démonstration les définitions, les théorèmes fondamentaux et les motivations de cette théorie, en insistant sur les outils dont je me suis servi par la suite. Je décris ensuite des résultats extraits des articles listés en §1.1 de ce mémoire. J'ai regroupé en deux catégories ces énoncés. Je regroupe sous l'intitulé "question de Kolster" ceux de mes résultats qui ont trait à la Λ-liberté des unités circulaires. Autant que je puisse en juger cette question est maintenant fermée. Je regroupe ensuite sous l'intitulé "classes d'idéaux et classes d'unités" les autres résultats ayant trait à la cyclotomie. Ce découpage est arbitraire et les deux chapitres sont connectés, même si l'absence de démonstration rend le lien moins apparent dans ce texte. Précisons ce lien maintenant. La majorité des résultats du chapitre 5 s'obtiennent par montée puis/ou par codescente dans une $\mathbb{Z}_p$-extension cyclotomique. Plusieurs auteurs (et j'en fais partie) ont cru pendant longtemps que la "question de Kolster" admettait une réponse positive. Et dans ce cas tous les processus de montée/descente avec les unités circulaires sont vraiment beaucoup plus simples. Comme la réponse à la question de Kolster est "en général non" les démonstrations et certains énoncés du chapitres 5 sont plus techniques.

L'article [BO01], numéroté 3 dans la liste d'articles parus, ne concerne pas la théorie d'Iwasawa cyclotomique. Faute de pouvoir l'insérer dans le corps de ce mémoire j'en dis quelques mots dans cette introduction. Dans cet article écrit avec Hassan Oukhaba, nous étudions une généralisation sur un corps de base arbitraire des distributions ordinaires universelles à la Kubert sur $\mathbb{Q}$. La compréhension (partielle) des distributions à la Kubert dans le cadre cyclotomique contient déjà toutes les informations dont on dispose sur la constante de Sinnott c décrite dans le §2.4 : c'est la démarche de Sinnott pour établir sa formule d'indices, et j'utiliserai souvent les distributions cyclotomiques dans ce mémoire. Pour les distributions attachées à (l'extension abélienne maximale) d'un corps de nombres arbitraire la simple question de l'existence d'un sous-groupe de torsion (non trivial) se posait. Nous avons donné des exemples pour lesquels ce sous-groupe est non trivial ce qui contredit une conjecture de Yin [Yin00]. En étendant à ce cadre certaines des techniques de [Bel98], et en utilisant des outils standards de cohomologie galoisienne, nous majorons ce sous-groupe lorsque le corps de base est un corps quadratique imaginaire. Cette majoration suffit pour les applications arithmétiques développées dans d'autres travaux d'Oukhaba. Nous donnons également des cas particuliers dans lesquels notre majoration est atteinte.

Chapitre 2

Unités circulaires.

2.1 Définition.

Depuis l'étude par Kummer de l'arithmétique du p-ième corps cyclotomique (p un nombre premier) et sa définition des unités cyclotomiques dans ce cas particulier, de nombreux auteurs (comprenant Leopoldt, Gillard, Washington, Sinnott, Thaine ...) ont proposé diverses versions "d'unités cyclotomiques" dans le but de généraliser cette définition pour des corps abéliens sur $\mathbb{Q}$ arbitraires. Trop de versions différentes, chacune avec ses avantages ont été proposées. On trouve dans la littérature des articles de bon niveau consacrés à la démonstration que telle variante coïncide avec telle autre. Pour ma part je pense qu'actuellement le module des unités circulaires à la Sinnott ([Sin80]), dont une définition suit, est la meilleure version disponible. Je crois aussi que ce module est optimal si l'on fait abstraction de la 2-partie de son indice dans les unités. On fixe F un corps de nombres absolument abélien totalement réel. On note $G = \mathrm{Gal}(F/\mathbb{Q})$ et $\mathrm{cond}(F)$ le conducteur de F. Pour tout $d \in \mathbb{N}$ on note $\zeta_d = \exp(2i\pi/d)$ la racine primitive d-ième complexe de l'unité. Pour tout $d \in \mathbb{N}$ on note

$$\varepsilon_{F,d} = N_{\mathbb{Q}(\zeta_d)/F\cap\mathbb{Q}(\zeta_d)}(1-\zeta_d).$$

L'entier algébrique $\varepsilon_{F,d}$ est une (ℓ)-unité si d est une puissance du nombre premier ℓ et est une unité si d est composé. Pour obtenir un système comprenant uniquement des unités il suffit de procéder comme suit. Pour tout ℓ et tout $s \in \mathbb{N}$ le groupe $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^s}) \cap F/\mathbb{Q})$ est cyclique (lorsque $\ell = 2$ on utilise le fait que F est totalement réel). On fixe un générateur $g_{l^s,F}$ de ce groupe. On note

$$\widetilde{\varepsilon}_{F,d} = \begin{cases} (\varepsilon_{F,l^s})^{1-g_{l^s,F}} \text{ si } d = \ell^s \\ \varepsilon_{F,d} \text{ si } d \text{ est composé.} \end{cases}$$

Même si les éléments $\widetilde{\varepsilon}_{F,d}$ dépendent des choix (non canoniques) des $g_{l^s,F}$, les modules galoisiens qu'ils engendrent n'en dépendent pas. Et tous les $\widetilde{\varepsilon}_{F,d}$ sont des unités.

Définition 2.1 ([Sin80]) *On appelle groupe des unités circulaires et l'on note C_F l'intersection du sous-$\mathbb{Z}[G]$-module de $F^\times$ engendré par -1 et les $\varepsilon_{F,d}$ pour $d \neq 1$ parcourant $\mathbb{N}$, avec le groupe des unités U_F de F.*

Cette définition est trivialement équivalente à celle de Sinnott qui fait intervenir les normes de nombres de la forme $1-(\zeta_n)^a$. Ces normes sont des puissances d'un conjugué par Galois de $\varepsilon_{F,d}$ pour $d = n/(a,n)$. Cette définition ne donne pas directement de système générateur fini explicite de C_F. Pour obtenir un tel système on doit utiliser les relations de distribution satisfaites par les nombres $1-\zeta_d$, que je rappelle tout de suite.

2.2 Relations de distribution.

Soit $d \in \mathbb{N}$ et soit ℓ un nombre premier divisant d. On note σ_l le Fröbenius arithmétique défini sur $\mathbb{Q}(\zeta_n)$ pour tout n non divisible par ℓ. Alors on a

$$N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}(\zeta_{d/\ell})}(1-\zeta_d) = \begin{cases} 1-\zeta_{d/\ell} \text{ si } \ell \mid d/\ell \\ \ell \text{ si } d = \ell \\ (1-\zeta_{d/\ell})^{(1-\sigma_\ell^{-1})} \text{ si } \ell \nmid d/\ell \text{ et } d \neq \ell \end{cases}$$

Ces formules permettent (à un 2-groupe abélien fini près) de décrire toutes les relations $\mathbb{Z}$-linéaires liant les $1-\zeta_d$ (voir [Bas66] corrigé et complété par [Enn72]). Elles permettent aussi de démontrer le lemme :

Lemme 2.2 *C_F est engendré comme $\mathbb{Z}[G]$-module par les $\widetilde{\varepsilon}_{F,d}$ si $d \neq 1$ parcourt l'ensemble des diviseurs de* $\mathrm{cond}(F)$.

Dans le cas particulier initialement étudié par Kummer le groupe des unités cyclotomiques de $\mathbb{Q}(\zeta_p)^+$ est non seulement un sous-groupe explicite de $\mathbb{Z}$-rang maximal des unités de $\mathbb{Q}(\zeta_p)^+$ mais satisfait aussi la formule d'indice :

$$(U_{\mathbb{Q}(\zeta_p)^+} : C_{\mathbb{Q}(\zeta_p)^+}) = \#\,\mathrm{Cl}(\mathbb{Q}(\zeta_p)^+)$$

où $\mathrm{Cl}(\mathbb{Q}(\zeta_p)^+)$ est le groupe des classes d'idéaux de $\mathbb{Q}(\zeta_p)^+$. En réalité les similarités entre $\mathrm{Cl}(\mathbb{Q}(\zeta_p)^+)$ et le quotient (appelons-le groupe des classes d'unités) $U_{\mathbb{Q}(\zeta_p)^+}/C_{\mathbb{Q}(\zeta_p)^+}$ dépassent largement l'égalité des ordres. Les définitions plus générales d'unités cyclotomiques se sont succédées et il s'agissait de trouver pour F abélien (totalement réel) quelconque un sous-module d'unités $\mathcal{E}_F$ tel que

1. $\mathcal{E}_F$ coïncide avec les unités cyclotomiques classiques lorsque F est (sous-corps réel maximal d'un corps) cyclotomique.
2. $\mathcal{E}_F$ soit explicitement défini.
3. $\mathcal{E}_F$ soit d'indice fini dans U_F et le quotient $U_F/\mathcal{E}_F$ soit lié (formules d'indice, d'indice raffinées, etc ...) au groupe des classes d'idéaux de F.

2.3 Formules analytiques.

La motivation initiale de l'étude des nombres de la forme $1-\zeta_d$ et la raison pour laquelle on s'attend à l'existence de sous-groupes d'unités cyclotomiques satisfaisant les propriétés 1 à 3 ci-dessus provient bien sûr des fonctions L de Dirichlet. Soit χ un caractère de Dirichlet *primitif* modulo f, soit $L(s,\chi)$ la fonction L qui prolonge la série de Dirichlet $s \mapsto \sum_{n\geq 1} \frac{\chi(n)}{n^s}$, et soit $\tau(\chi) = \sum_{a=1}^{a=f} \chi(a)\zeta_f^a$, la somme de Gauß classique.

Théorème 2.3 ([Was97] theorem 4.9) *Si* $\chi(-1) = 1$ *alors*

$$L(1,\chi) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \chi(a)^{-1} \log\left|1-\zeta_f^a\right|$$

Via l'équation fonctionnelle la formule du théorème 2.3 conduit à

Corollaire 2.4 *Si* $\chi(-1) = 1$ *alors*

$$L'(0,\chi) = -\frac{1}{2} \sum_{a=1}^{f} \chi(a) \log\left|1-\zeta_f^a\right|$$

Cette formule montre que l'unité cyclotomique $1-\zeta_f$ est une unité de Stark sur $\mathbb{Q}$ au sens de Tate ([Tat84], chapitre III§5 et chapitre IV). Le seul autre cas non trivial connu d'existence de telles unités est fourni par les unités elliptiques (au dessus d'un corps quadratique imaginaire) avec la "seconde formule limite de Kronecker" (analogue de celle du corollaire 2.4).

Ces formules sont à comparer avec la formule analytique du nombre de classes. Soit $\zeta_F(s)$ la fonction zeta de Dedekind associée au corps abélien F, et soit $\widehat{G}$ le groupe des caractères de Dirichlet associé à F. Alors $\zeta_F(s) = \prod_{\chi\in\widehat{G}} L(s,\chi)$.

Théorème 2.5 *Soit F un corps de nombres totalement réel*[1]*. Soit $[F:\mathbb{Q}]$ le degré de F sur $\mathbb{Q}$, R le régulateur de Dirichlet de F, et $h = \#\,\mathrm{Cl}(F)$ le nombre de classes d'idéaux de F. Alors ζ_F a un zéro d'ordre $[F:\mathbb{Q}]-1$ en $s=0$ et on a*

$$\lim_{s\to 0} \frac{\zeta_F(s)}{s^{[F:\mathbb{Q}]-1}} = \frac{hR}{2}$$

Avec cette formule, connue sous le nom de "formule analytique du nombre de classe", on peut considérer qu'on connaît explicitement le produit hR. Un problème fondamental dans la théorie des nombres est de séparer le nombre entier h de la quantité transcendante R. Naïvement on pourrait espérer déduire une expression explicite pour R à partir d'une expression explicite d'un système fondamental d'unités de F. Bien sûr on ne sait pas expliciter un tel système en général. De là provient l'intérêt de systèmes générateurs dans le goût de ceux du lemme 2.2. En effet la formule du corollaire 2.4 s'interprète alors comme le calcul de la χ-partie d'un régulateur cyclotomique et conduit à une formule d'indice (dans laquelle naturellement le nombre de classes d'idéaux réapparaît). C'est l'esprit de la démonstration de la formule d'indice de Sinnott que je rappelle maintenant.

2.4 Indice des unités circulaires.

Théorème 2.6 ([Sin80]) *Soit c_F la constante de Sinnott de F, alors*

$$(U_F : C_F) = c_F h_F.$$

Pour que ce théorème ait un contenu on doit définir la constante c_F indépendamment de cette égalité. Soit $\mathbb{Z}[G]$ l'algèbre de groupe et soit $Iw(F)$ le sous-$\mathbb{Z}[G]$-module de $\mathbb{Q}[G]$ noté U dans [Sin80] et redéfini dans la définition 2.1 de [BN01]. Alors on a :

$$c_F = 2^{[F:\mathbb{Q}]-1} \frac{\prod_l [F\cap\mathbb{Q}(\zeta_{l^\infty}):\mathbb{Q}]}{[F:\mathbb{Q}]} (\mathbb{Z}[G] : Iw(F))$$

Il est possible de corriger la définition de C_F pour supprimer le facteur $2^{[F:\mathbb{Q}]-1}$. La constante "dure" et techniquement difficile est l'indice généralisé $(\mathbb{Z}[G] : Iw(F))$. Le réseau $Iw(F)$ apparaît dans le contexte plus général des distributions ordinaires universelles attachées (à la théorie du corps de classes) d'un corps global. En effet c'est le module noté I dans [Yin00] et étudié sous le nom de distribution d'Iwasawa dans [BO01]. L'essentiel du

[1] La formule analytique du nombre de classes est vraie en toute généralité, mais pour éviter d'introduire des notations supplémentaires je suppose que F est totalement réel.

travail technique de l'article [Sin80] consiste à "contrôler" la constante c_F. En raisonnant nombre premier par nombre premier, on sait par exemple que si p est impair et ne divise pas $[F : \mathbb{Q}]$ alors p ne divise pas non plus c_F. Disons pour simplifier que l'ordre du groupe des classes d'unités U_F/C_F est essentiellement égal à celui du groupe des classes d'idéaux $\mathrm{Cl}(F)$ de F. Si l'on interprète (et on verra que c'est là le bon point de vue) la collection des unités cyclotomiques comme des incarnations "algébriques" de la collection des fonctions L de Dirichlet, cette formule d'indice doit être vue comme la traduction algébrique de la formule analytique du nombre de classes.

2.5 Une conjecture de Gras.

Fixons un nombre premier p et pour tout $\mathbb{Z}[G]$-module M notons $\overline{M}$ le $\mathbb{Z}_p[G]$-module obtenu par pro-p-complétion à partir de M, autrement dit

$$\overline{M} = \lim_{\leftarrow\, n\in\mathbb{N}} M/p^n M.$$

Lorsque $p \nmid [F : \mathbb{Q}]$, puisque $p \nmid c_F$, la formule d'indice de Sinnott donne l'égalité des ordres des p-adifiés $\overline{U_F/C_F}$ et $\overline{\mathrm{Cl}(F)}$. Dans un premier temps on pourrait espérer que cette égalité provienne d'un isomorphisme entre ces deux modules galoisiens. Cela ne se peut pas puisque par exemple pour les corps quadratiques réels, le groupe U_F/C_F est cyclique tandis que le p-rang de $\mathrm{Cl}(F)$ peut-être rendu arbitrairement grand. En cherchant des similarités moins fortes entre les p-adifiés de ces deux groupes de classes, Gras a conjecturé que les $\mathbb{Z}_p[G]$-modules $\overline{U_F/C_F}$ et $\overline{\mathrm{Cl}(F)}$ ont les mêmes invariants de Jordan-Hölder. Cette conjecture est équivalente à l'égalité des ordres des χ-composantes des deux $\mathbb{Z}_p[G]$-modules pour tout $\chi \in \widehat{G}$. Grâce à Greenberg on sait que la conjecture principale de la théorie d'Iwasawa entraîne la conjecture de Gras. Dans le contexte présent la conjecture principale est un théorème de Mazur et Wiles, puis Wiles (voir [MW84] et [Wil90]). En utilisant la Conjecture Principale et en suivant une démarche par co-descente très technique, Kuz′Min ([Kuz96]) a démontré une généralisation de la conjecture de Gras pour des corps abéliens réels F quelconques (y compris ceux de degré divisible par p). Dans les deux premières parties de [BN01], je re-démontre le résultat de Kuz′Min. J'utilise aussi la Conjecture Principale mais l'essentiel de la démonstration a lieu au niveau fini. Cette approche est sensiblement plus simple que celle de Kuz′min mais utilise elle aussi le point de vue p-adique et la théorie d'Iwasawa que je décris dans le prochain chapitre.

Chapitre 3

Théorie d'Iwasawa.

L'objet de ce chapitre est de passer en revue des notions classiques de théorie d'Iwasawa, relevant de la théorie algébrique ou de l'analyse p-adique, pour arriver à formuler la version de la Conjecture Principale (théorème de Mazur-Wiles et Wiles dans le cadre qui nous intéresse) qui est l'un des outils les plus puissants de l'arithmétique contemporaine.

3.1 Généralités algébriques.

Soit p un nombre premier impair fixé[1]. La théorie d'Iwasawa a pour objet l'arithmétique des $\mathbb{Z}_p$-extensions (éventuellement des $(\mathbb{Z}_p)^s$-extensions). Soit K un corps de nombres et K_∞/K une $\mathbb{Z}_p$-extension. On utilise les notations habituelles suivantes $\Gamma := \mathrm{Gal}(K_\infty/K)$, $\Gamma_n := \Gamma^{p^n}$, $G_n := \Gamma/\Gamma_n$, $K_n := K_\infty^{\Gamma_n}$, et $\Lambda := \mathbb{Z}_p[[\Gamma]]$ est l'algèbre d'Iwasawa usuelle. Le choix d'un générateur topologique γ de Γ permet d'identifier Λ à l'anneau $\mathbb{Z}_p[[T]]$ des séries formelles à une indéterminée à coefficients dans $\mathbb{Z}_p$, en posant $\gamma = T + 1$. Étant donnée une suite $(M_n)_{n\in\mathbb{N}}$ de $\mathbb{Z}_p[G_n]$-modules munie de morphismes de norme G_{n+1}-équivariant $N_{n+1,n}\colon M_{n+1} \longrightarrow M_n$, on obtient par passage à la limite projective un Λ-module $M_\infty = \varprojlim_n M_n$. De tels modules sont classifiés à pseudo-isomorphisme près de la même façon que les modules sur les anneaux principaux (à isomorphisme près).

Définition 3.1 *On dit qu'un morphisme de Λ-module $f\colon M \longrightarrow N$ est un pseudo-isomorphisme lorsque* $\ker f$ *et* $\mathrm{Coker}\, f$ *sont finis.*

Définition 3.2 *Un polynôme $P(T) = T^n + \sum_{k=1}^{k=n} a_k T^k \in \mathbb{Z}_p[T]$ est dit distingué lorsque $p \mid a_k$ pour tout $k \neq n$.*

[1] La théorie d'Iwasawa s'énonce aussi pour $p = 2$. Mais cela simplifie considérablement la partie technique de l'exposé de supposer $p \neq 2$.

Théorème 3.3 *Soit M_∞ un Λ-module de type fini. Il existe r, s, et $t \in \mathbb{N}$; des polynômes distingués $(f_j)_{j=1}^{j=t}$ de $\mathbb{Z}_p[T]$; des entiers $(n_i)_{i=1}^{i=s}$, des entiers $(m_j)_{j=1}^{j=t}$ et un pseudo-isomorphisme f de Λ-modules*

$$f\colon M_\infty \longrightarrow \Lambda^r \bigoplus \left(\bigoplus_{i=1}^{i=s} \frac{\Lambda}{(p^{n_i})} \right) \bigoplus \left(\bigoplus_{j=1}^{j=t} \frac{\Lambda}{(f_j(T)^{m_j})} \right)$$

Ce théorème permet d'associer à tout Λ-module de type fini les fameux invariants d'Iwasawa.

Définition 3.4 *Soit M_∞ un Λ-module de type fini. On reprend les notations du théorème 3.3.*

1. *On appelle invariants ρ, λ et μ d'Iwasawa les quantités*

$$\rho = r, \quad \lambda = \sum_{j=1}^{j=t} m_j \deg(f_j(T)), \quad \mu = \sum_{i=1}^{i=s} n_i.$$

2. *Si M_∞ est de torsion on appelle polynôme caractéristique de M_∞ et on note $\mathrm{car}(M)$ le polynôme*

$$\mathrm{car}(M) = p^\mu \prod_{j=1}^{j=t} f_j(T)^{m_j}.$$

Le théorème 3.3 reste vrai et la notion de polynôme caractéristique (définition 3.4.2) subsiste si l'on remplace $\mathbb{Z}_p[[\Gamma]]$ par $\mathcal{O}[[\Gamma]]$ pour tout $\mathcal{O}$ anneau d'entiers sur $\mathbb{Z}_p$ d'une extension finie de $\mathbb{Q}_p$ (éventuellement on doit remplacer p par une uniformisante de $\mathcal{O}$). Bien entendu l'invariant naturel n'est pas le polynôme $\mathrm{car}(M)$ mais l'idéal caractéristique $(\mathrm{car}(M))$ qu'il engendre. Cet idéal se comporte vis-à-vis des suites exactes de Λ-modules de torsion de type fini comme une caractéristique d'Euler-Poincaré (multiplicativement). Les invariants λ et μ sont utilisés dans les formules asymptotiques.

Proposition 3.5 *Soit M_∞ un Λ-module de torsion tel que $\mathrm{car}(M_\infty)$ soit sans facteur commun avec tous les $(T+1)^{p^n} - 1$ pour $n \in \mathbb{N}$, et soit λ et μ les invariants d'Iwasawa de M_∞. Alors pour tout n, l'ordre des Γ_n-co-invariants $\#(M_\infty)_{\Gamma_n}$ est fini. En outre, il existe $N \in \mathbb{N}$ et $\nu \in \mathbb{Z}$ tels que pour tout $n \geq N$ on ait*

$$\#(M_\infty)_{\Gamma_n} = p^{\mu p^n + \lambda n + \nu}.$$

Dans l'esprit des formules asymptotique mentionnons ici le fameux théorème d'Iwasawa (même si sa nature est plus arithmétique que celle des autres énoncés de cette section). Pour tout n on note $X_n = \overline{\mathrm{Cl}(K_n)}$ la p-partie du groupe des classes de K_n et on forme le Λ-module $X_\infty := \varprojlim X_n$.

Théorème 3.6 *Soient λ et μ les invariants associés à X_∞. Alors il existe $N \in \mathbb{N}$ et $\nu \in \mathbb{Z}$ tels que pour tout $n \geq N$ on ait*

$$\#X_n = p^{\mu p^n + \lambda n + \nu}.$$

Les énoncés 3.5 et 3.6 sont similaires. On pourrait croire que le théorème 3.6 se déduit directement de la proposition 3.5 par comparaison entre $(X_\infty)_{\Gamma_n}$ et X_n. Il n'en est rien et d'ailleurs la démonstration d'Iwasawa qui est parallèle à la démonstration classique de la proposition 3.5, est valable en toute généralité, même pour des extensions K_∞/K pour lesquelles on ne sait pas démontrer la finitude des co-invariants $(X_\infty)_{\Gamma_n}$.

3.2 Fonctions L de Kubota-Leopoldt.

On connaît à ce jour (au moins) trois façons différentes de construire les fonctions L p-adiques de Kubota-Leopoldt. Je les rappelle brièvement en suivant essentiellement l'exposé de [Iwa72] pour les deux premières constructions et de [Tsu99] et [Tsu01] pour la troisième construction. On fixe définitivement et simultanément un plongement de la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ dans le corps des nombres complexes $\mathbb{C}$ et dans le corps de Tate $\mathbb{C}_p$. Ces plongements définissent le caractère de Teichmüller $\omega\colon \mathbb{Z} \longrightarrow \overline{\mathbb{Q}}$ et permettent de comparer les valeurs algébriques des fonctions analytiques complexes et p-adiques.

3.2.1 Interpolation p-adique.

Soit χ un caractère de Dirichlet primitif modulo f. On suppose une fois pour toutes $\chi(-1) = 1$, cela évite de construire des fonctions L_p identiquement nulles. Soit $F_\chi(s)$ la fonction analytique complexe

$$F_\chi(s) = \sum_{a=1}^{f} \frac{\chi(a) s e^{as}}{e^{fs} - 1}.$$

On définit les nombres de Bernoulli généralisés $B_{n,\chi} \in \mathbb{Q}(\zeta_f)$ à partir du développement de Taylor de F_χ, c'est-à-dire comme vérifiant la formule

$$F_\chi(s) = \sum_{n \in \mathbb{N}} B_{n,\chi} \frac{s^n}{n!}.$$

La motivation pour introduire ces nombres algébriques est le théorème suivant.

Théorème 3.7 *Pour tout entier $n \geq 1$ on a*

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}.$$

La fonction $L_p(-,\chi)$ de Kubota et Leopoldt a été définie historiquement comme une sorte de compromis p-adiquement analytique entre les $p-1$ fonctions de la variable complexe $(1-\chi\omega^n(p)p^{-s})L(s,\chi\omega^n)$, $n = 0, \cdots, p-1$.

Théorème 3.8 *Il existe une unique fonction $L_p(-,\chi)$ méromorphe (holomorphe si $f \neq 1$) sur $\{s \in \mathbb{C}_p \,\big|\, |s| < pp^{-1/(p-1)}\}$ telle que pour tout $n \geq 1$:*

$$L_p(1-n,\chi) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n} = (1-\chi\omega^{-n}(p)p^{n-1})L(1-n,\chi\omega^{-n})$$

L'existence de cette fonction est donnée par un développement de Mahler (en $1-s$) dans [Was97] theorem 5.11, par exemple. Lorsque $f = 1$ la seule singularité est en $s = 1$: on retrouve le pôle d'ordre 1 de la fonction zeta de Riemann. Pour χ non trivial la valeur en 1, qui n'est pas décrite par la formule de définition, joue un rôle très important dans la présente approche. La formule du théorème 2.3 reste valable telle quelle dans le monde p-adique (en remplaçant fonction L par L_p et logarithme complexe log par le logarithme d'Iwasawa $\log_p$). Je rappelle qu'on a fixé définitivement des plongements de $\overline{\mathbb{Q}}$ dans $\mathbb{C}_p$ et $\mathbb{C}$, sans lesquels la formule qui suit n'aurait absolument aucun sens.

Théorème 3.9 (theorem 5.18 of [Was97]) *Si $f \neq 1$ alors*

$$L_p(1,\chi) = -\left(1-\frac{\chi(p)}{p}\right)\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\chi(a)^{-1}\log_p\left(1-\zeta_f^a\right)$$

Mentionnons dès maintenant que la conjecture de Leopoldt pour $\mathbb{Q}(\zeta_f)$ est équivalente à $L_p(1,\chi) \neq 1$ pour tout χ pair non trivial de conducteur divisant f. La seconde construction de cette même fonction p-adique est due à Iwasawa et définit la série formelle qui intervient dans la conjecture principale.

3.2.2 Série d'Iwasawa.

On reprend, sans les démonstrations, la démarche exposée dans [Iwa72] §6 et [Was97] §7 ; en essayant autant que possible de simplifier les notations.

On a fixé un caractère de Dirichlet χ pair et primitif modulo f. On factorise $f = dp^j$ avec $p \nmid d$. On note $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_{dp})/\mathbb{Q})$ et pour tout n on note $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{dp^{n+1}})/\mathbb{Q}(\zeta_{dp}))$. Pour tout n le groupe $\mathrm{Gal}(\mathbb{Q}(\zeta_{dp^{n+1}})/\mathbb{Q})$ s'identifie au produit $\Delta \times G_n$ et il en va de même pour les groupes de caractères $\widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_{dp^{n+1}})/\mathbb{Q})} = \widehat{\Delta} \times \widehat{G}_n$. Pour tout $a \in \mathbb{Z}$ tel que $(a, dp) = 1$ on définit $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_{dp^{n+1}})/\mathbb{Q})$ par $\sigma_a(\zeta_{dp^{n+1}}) = \zeta_{dp^{n+1}}^a$. En accord avec les décompositions ci-dessus on note $\sigma_a = \delta(a)\gamma_n(a)$ avec $\delta(a) \in \Delta$ et $\gamma_n(a) \in G_n$; et dès que $n \geq j-1$ on peut voir χ comme un caractère modulo dp^{n+1} et écrire $\chi = \theta\psi$ avec $\theta \in \widehat{\Delta}$ et ψ trivial ou $\psi \in \widehat{G}_{j-1}$. On dit alors que θ (de conducteur divisant dp) est un caractère de première espèce et que ψ (d'ordre une puissance de p et de conducteur divisant p^j) est un caractère de seconde espèce. Les caractères de seconde espèce décrivent les représentations de G_n. Avec le théorème de classification on a vu comment la théorie algébrique d'Iwasawa permet de "trivialiser" l'action de Galois de G_n. Au contraire l'action de Δ, surtout lorsque $p \mid \#\Delta$, requiert un traitement nettement plus fin (dans le goût des conjectures principales équivariantes, voir par exemple [RW02, BG03]).

Pour tout n on part de l'élément de Stickelberger ξ_n associé aux fonctions ζ partielles de l'extension $\mathbb{Q}(\zeta_{dp^{n+1}})/\mathbb{Q}$:

$$\begin{aligned}\xi_n &= \frac{1}{dp^{n+1}} \sum_{(a,dp)=1,\, a=1}^{a=p^{n+1}} \left(\frac{dp^{n+1}}{2} - a\right) \sigma_a^{-1} \\ &= \sum_{(a,dp)=1,\, a=1}^{a=p^{n+1}} \zeta(\sigma_a, 0)\sigma_a^{-1} \quad \in \mathbb{Q}[\Delta \times G_n].\end{aligned}$$

Il est plus commode de raisonner en chassant le dénominateur p-adique de ξ_n et pour ce on introduit aussi :

$$\eta_n = (1 - (1+dp)\gamma_n(1+dp)^{-1})\xi_n.$$

L'étape suivante consiste à projeter η_n et ξ_n sur la composante isotypique associée au caractère miroir $\theta^* = \omega\theta^{-1}$ de θ. Soit $\varepsilon_{\theta^*} = \dfrac{1}{\#\Delta} \displaystyle\sum_{\delta \in \Delta} \theta^*(\delta)\delta^{-1}$ l'idempotent de $\mathbb{C}_p[\Delta]$ associé à θ^*. Alors il existe un unique $\xi_n(\theta)$ et un unique $\eta_n(\theta)$ dans $\mathbb{Q}_p(\theta)[G_n]$ tels que $\varepsilon_{\theta^*}\xi_n = \xi_n(\theta)\varepsilon_{\theta^*}$ et $\varepsilon_{\theta^*}\eta_n = \eta_n(\theta)\varepsilon_{\theta^*}$.

Proposition 3.10 ([Was97] proposition 7.6)

1. $\frac{1}{2}\eta_n(\theta) \in \mathbb{Z}_p[\theta][G_n]$.
2. *Si θ est non trivial alors* $\frac{1}{2}\xi_n(\theta) \in \mathbb{Z}_p[\theta][G_n]$.

3. *Si $m \geq n \geq 0$ alors $\eta_m(\theta)$ (respectivement $\xi_m(\theta)$) s'envoie sur $\eta_n(\theta)$ (respectivement $\xi_n(\theta)$) par l'application de restriction $G_m \twoheadrightarrow G_n$.*

On pose $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_{dp^\infty})/\mathbb{Q}(\zeta_{dp}) = \lim G_n$. Cette proposition montre qu'on obtient par passage à la limite deux éléments

$$\xi_\infty(\theta) = \lim(\xi_n(\theta)) \in \mathbb{Q}_p(\theta)[[\Gamma]] \quad \text{et} \quad \eta_\infty(\theta) = \lim(\eta_n(\theta)) \in \mathbb{Z}_p[\theta][[\Gamma]],$$

avec dans $\xi_\infty(\theta) \in \mathbb{Z}_p[\theta][[\Gamma]]$ si θ est non trivial.

Pour obtenir les séries d'Iwasawa il suffit maintenant de spécifier le bon choix d'isomorphisme $\mathbb{Z}_p[\theta][[\Gamma]] \cong \mathbb{Z}_p[\theta][[T]]$. Soit

$$\gamma_\infty(1+dp) = \lim(\gamma_n(1+dp)).$$

Alors $\gamma_\infty(1+dp)$ engendre Γ et il existe un unique isomorphisme d'anneaux $\alpha\colon \mathbb{Z}_p[\theta][[\Gamma]] \longrightarrow \mathbb{Z}_p[\theta][[T]]$ tel que $\alpha(\gamma_\infty(1+dp)) = 1+T$. On peut maintenant définir les séries d'Iwasawa :

Définition 3.11 *On pose*

$$h(T,\theta) = 1 - \frac{1+dp}{1+T} \in \mathbb{Z}_p[\theta][[T]].$$

$$g(T,\theta) = \alpha(\eta_\infty(\theta)) \in \mathbb{Z}_p[\theta][[T]].$$

$$f(T,\theta) = \begin{cases} \alpha(\xi_\infty(\theta)) \in \mathbb{Z}_p[\theta][[T]] \text{ si } \theta \text{ est non trivial.} \\ \dfrac{g(T,\theta)}{h(T,\theta)} \in \mathbb{Q}_p(\theta)[[T]] \text{ sinon.} \end{cases}$$

Remarquons que pour tout θ on a $g(T,\theta) = h(T,\theta)f(T,\theta)$. C'est la série $f(T,\theta)$ qu'on voulait définir dans cette section. Cette série permet de formuler (une des versions de) la conjecture principale et redonne les fonctions L_p par le théorème :

Théorème 3.12 *Soit $\chi = \theta\psi$ un caractère de Dirichlet pair avec θ de première espèce et ψ de seconde espèce. On pose $\zeta_\chi = \chi(1+dp)^{-1}$. Alors pour tout $s \in \mathbb{C}_p$ avec $|s| < pp^{-1/(p-1)}$ et $s \neq 1$ si χ est trivial on a*

$$L_p(s,\chi) = f(\zeta_\chi(1+dp)^s - 1, \theta).$$

Le facteur ψ de seconde espèce intervient uniquement à travers la racine de l'unité $\zeta_\chi = \chi(1+dp)^{-1} = \psi(1+dp)^{-1}$. En particulier pour retrouver les fonctions L_p il suffit de construire les séries $f(T,\theta)$ associées aux caractères de première espèce : c'est le pendant analytique de la trivialisation de l'action de Γ vu dans le paragraphe 3.1.

3.2.3 Morphisme de Coleman et élément cyclotomique.

Cette troisième construction est plus récente que les deux précédentes. Elle est due à Coleman [Col83] dans le cas particulier où le caractère étudié est de la forme ω^i. Le cas général est traité par T. Tsuji dans [Tsu99] §4. Essentiellement on retrouve la série formelle $f(T,\theta)$ en appliquant à un élément cyclotomique bien choisi le morphisme de Coleman ([Col79]). On commence par rappeler la définition de ce morphisme (pour le groupe formel multiplicatif). On fixe un caractère θ de première espèce. Ce n'est pas une restriction de généralité pour le problème qui nous concerne : voir le §3.2.2. Le conducteur de θ est égal à d ou à dp avec $p \nmid d$. Soit $\mathbb{B}_\infty/\mathbb{Q}$ la $\mathbb{Z}_p$-extension de $\mathbb{Q}$. On reprend les notations de [Tsu99] : on note $F = \mathbb{Q}(\zeta_d)$, $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, $G_0 = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, et pour $n \geq 0$ on note $K_n = \mathbb{Q}(\zeta_{dp^{n+1}})$ et $\Gamma = \mathrm{Gal}(\mathbb{B}_\infty/\mathbb{Q})$. Le groupe $\mathrm{Gal}(K_\infty/\mathbb{Q})$ se décompose canoniquement en produit direct $\mathrm{Gal}(K_\infty/\mathbb{Q}) = \Gamma \times \Delta \times G_0$. Soit $\mathfrak{P}$ une place de F divisant p et soit $\Delta_\mathfrak{P} = \mathrm{Gal}(F_\mathfrak{P}/\mathbb{Q}_p)$ le sous-groupe de décomposition en $\mathfrak{P}$. Le Fröbenius σ_p est ainsi un élément bien défini de $\Delta_\mathfrak{P} \subset \Delta \subset \mathrm{Gal}(K_\infty/\mathbb{Q})$. Pour tout $\mathbb{Z}_p[\Delta_\mathfrak{P}]$-module M on notera $\mathrm{Ind}_\mathfrak{P}(M)$ le $\mathbb{Z}_p[\Delta]$-module induit :

$$\mathrm{Ind}_\mathfrak{P}(M) = M \otimes_{\mathbb{Z}_p[\Delta_\mathfrak{P}]} \mathbb{Z}_p[\Delta].$$

Soit $\kappa\colon \Gamma \times G_0 \longrightarrow \mathbb{Z}_p^\times$ le "caractère" cyclotomique et soit $\mathcal{O}_\mathfrak{P}$ l'anneau de valuation de $F_\mathfrak{P}$. Le groupe $\Delta_\mathfrak{P}$ agit via les coefficients sur l'anneau de séries formelles $\mathcal{O}_\mathfrak{P}[[X]]$. On définit une action de Γ et G_0 sur $\mathcal{O}_\mathfrak{P}[[X]]$ par la formule :

$$(\tau f)(X) = f((1+X)^{\kappa(\tau)} - 1).$$

Soit $\mathcal{M}_\mathfrak{P} := \{f(X) \in \mathcal{O}_\mathfrak{P}[[X]] \,|\, f(0) \equiv 1[p]\}$. Pour les actions définies ci-dessus, le groupe multiplicatif $\mathcal{M}_\mathfrak{P}$ et le groupe additif $\mathcal{O}_\mathfrak{P}[[X]]$ sont des modules topologiques sur $\mathbb{Z}_p[[\Delta_\mathfrak{P} \times G_0 \times \Gamma]]$. Soit $\mathcal{N}\colon \mathcal{O}_\mathfrak{P}((X))^\times \longrightarrow \mathcal{O}_\mathfrak{P}((X))^\times$ l'opérateur norme de Coleman caractérisé par

$$(\mathcal{N}f)((1+X)^p - 1) = \prod_{\zeta^p=1} f(\zeta(1+X) - 1).$$

Théorème 3.13 ([Tsu99] theorem 4.1) *Soit $\alpha = (\alpha_n)_{n\geq 0}$ une suite cohérente en norme dans $\lim_n F_\mathfrak{P}(\zeta_{p^{n+1}})^\times$. Alors il existe une unique série formelle $f_\alpha \in \mathcal{O}_\mathfrak{P}((X))^\times$ telle que :*

$$f_\alpha(\zeta_{p^{n+1}} - 1) = (\alpha_n)^{(\sigma_p)^n} \qquad et \qquad \mathcal{N}f_\alpha = (f_\alpha)^{\sigma_p}.$$

Soit $U^1_{\mathfrak{P},\infty}$ la limite projective des unités principales $U^1_{\mathfrak{P},n}$ des $F_\mathfrak{P}(\zeta_{p^{n+1}})$, et soit $\mathcal{M}^{\mathcal{N}=\sigma_p} := \{f \in \mathcal{M} \,|\mathcal{N}f = f^{\sigma_p}\}$. L'application $\alpha \mapsto f_\alpha$ est un $\mathbb{Z}_p[[\Delta_\mathfrak{P} \times G_0 \times \Gamma]]$-isomorphisme

$$U^1_{\mathfrak{P},\infty} \xrightarrow{\sim} \mathcal{M}^{\mathcal{N}=\sigma_p}.$$

Soit φ l'endomorphisme continu de $\mathcal{O}_{\mathfrak{P}}[[X]]$ défini par

$$(\varphi f)(X) = f^{\sigma_p}((1+X)^p - 1).$$

La formule

$$\Psi(f(X)) = \left(1 - \frac{\varphi}{p}\right)\log(f(X))$$

définit un $\mathbb{Z}_p[[\Delta_{\mathfrak{P}} \times G_0 \times \Gamma]]$-morphisme $\Psi\colon \mathcal{M} \longrightarrow \mathcal{O}_{\mathfrak{P}}[[X]]$. De plus l'image par Ψ de $\mathcal{M}^{\mathcal{N}=\sigma_p}$ est contenue dans le $\mathcal{O}_{\mathfrak{P}}[[G_0 \times \Gamma]]$-module libre engendré par $(1+X)$:

$$\Psi(\mathcal{M}^{\mathcal{N}=\sigma_p}) = \mathcal{O}_{\mathfrak{P}}[[G_0 \times \Gamma]](1+X).$$

Définition 3.14 *La formule*

$$\Psi(f_u(X)) = \mathrm{Col}_{\mathfrak{P}}(u)(1+X)$$

définit un $\mathbb{Z}_p[[\Delta_{\mathfrak{P}} \times G_0 \times \Gamma]]$*-morphisme*

$$\mathrm{Col}_{\mathfrak{P}}\colon U^1_{\mathfrak{P},\infty} \longrightarrow \mathcal{O}_{\mathfrak{P}}[[G_0 \times \Gamma]].$$

On note $\mathbb{Z}_p(1) \subset U^1_{\mathfrak{P},\infty}$ la limite projective des racines de l'unité. Le morphisme $\mathrm{Col}_{\mathfrak{P}}$ détermine complètement la structure de $U^1_{\mathfrak{P},\infty}$ grâce au théorème suivant.

Théorème 3.15 ([Tsu99] theorem 4.2) *On a une suite exacte :*

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow U^1_{\mathfrak{P},\infty} \xrightarrow{\mathrm{Col}_{\mathfrak{P}}} \mathcal{O}_{\mathfrak{P}}[[G_0 \times \Gamma]] \xrightarrow{\kappa} \mathbb{Z}_p(1) \longrightarrow 0$$

On note Col le morphisme obtenu à partir de $\mathrm{Col}_{\mathfrak{P}}$ par induction de $\Delta_{\mathfrak{P}}$ à Δ. On obtient ainsi la suite exacte :

$$\mathrm{Ind}_{\mathfrak{P}}(\mathbb{Z}_p(1)) \hookrightarrow \mathrm{Ind}_{\mathfrak{P}}(U^1_{\mathfrak{P},\infty}) \xrightarrow{\mathrm{Col}} \mathrm{Ind}_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}})[[G_0 \times \Gamma]] \xrightarrow{\kappa} \mathrm{Ind}_{\mathfrak{P}}(\mathbb{Z}_p(1))\ .$$

Le morphisme Col s'étend de manière unique en un homomorphisme

$$\mathrm{Col}\colon\ \mathrm{Ind}_{\mathfrak{P}}(\varprojlim_n F_{\mathfrak{P}}(\zeta_{p^{n+1}})^\times) \longrightarrow \mathrm{Ind}_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}})[[G_0 \times \Gamma]]^\sim,$$

où $\mathrm{Ind}_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}})[[G_0 \times \Gamma]]^\sim$ désigne l'ensemble des éléments f du corps des fractions de $\mathrm{Ind}_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}})[[G_0 \times \Gamma]]$ vérifiant $(\tau - 1)f \in \mathrm{Ind}_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}})[[G_0 \times \Gamma]]$ pour tout $\tau \in G_0 \times \Gamma$. Pour tout n on note

$$U'_n := \{x \in F(\zeta_{p^{n+1}})^\times \,|v(x) = 0 \text{ en toute place finie } v \nmid p \text{ de } F(\zeta_{p^{n+1}})\},$$

le module galoisien des (p)-unités, on note $\overline{U}'_n$ le pro-p-complété de $\overline{U}'_n$ et $\overline{U}'_\infty$ la limite projective (pour les applications de norme) des $\overline{U}'_n$. Le morphisme "diagonal" $\mathrm{diag}\colon \overline{U}'_\infty \longrightarrow \mathrm{Ind}_{\mathfrak{P}}(\lim_n F_{\mathfrak{P}}(\zeta_{p^{n+1}})^\times)$ est connu pour être injectif (c'est une version "faible" de la conjecture de Leopoldt). On choisit l'élément cyclotomique suivant :

$$\begin{aligned}\eta_d = \mathrm{diag}((1-\zeta_{p^{n+1}}\zeta_d^{\sigma_p{}^{-n}})_{n\in\mathbb{N}}) &= \mathrm{diag}((\sigma_{(p,d)}(1-\zeta_{dp^{n+1}}))_{n\in\mathbb{N}})\\ &\in \mathrm{Ind}_{\mathfrak{P}}(\lim_n F_{\mathfrak{P}}(\zeta_{p^{n+1}})^\times).\end{aligned}$$

Où $\sigma_{(p,d)}$ est l'unique élément de $G_0\times\Delta\times\Gamma$ vérifiant $\sigma_{(p,d)}(\zeta_{p^n})=\zeta_{p^n}^d$ pour tout n et $\sigma_{(p,d)}(\zeta_d)=\zeta_d^p$. Pour tout générateur γ de Γ on note $\alpha_\gamma\colon \mathbb{Z}_p[[\Gamma]]\longrightarrow \mathbb{Z}_p[[T]]$ l'isomorphisme défini par $\gamma\mapsto T+1$. Alors $\alpha_\gamma(\mathrm{Col}(\eta_d))$ est une série de Laurent bien définie. En fait $\alpha_\gamma(\mathrm{Col}(\eta_d))\in (1/T)\,\mathrm{Ind}_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}})[G_0][[T]]$ et même $\alpha_\gamma(\mathrm{Col}(\eta_d))\in \mathrm{Ind}_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}})[G_0][[T]]$ si $d>1$. Comme pour la série de Stickelberger on doit projeter cette série sur une composante θ-isotypique. Pour ce on est contraint de choisir un générateur (canonique ?) de cette "θ-composante". Soit

$$e_\theta = (p-1)^{-1}\sum_{g\in\Delta\times G_0}\theta(g)g^{-1}\in\mathbb{Z}_p[\theta][\Delta\times G_0],$$

le pseudo-idempotent associé à θ. Alors pour tout $x\in\mathrm{Ind}_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}})[G_0]\otimes\mathbb{Z}_p[\theta]$, il existe un unique $\widetilde{x}_\theta\in\mathbb{Z}_p[\theta]$ tel que $e_\theta x=\widetilde{x}_\theta e_\theta(\zeta_d\otimes 1)$ (c'est une conséquence du lemme 5.1 de [Tsu99] par exemple).

Proposition et définition 3.16 *Il existe une unique série formelle*

$$g_{\theta,\gamma}(T)\in\frac{1}{T}\mathbb{Z}_p[\theta][[T]],\ \textit{telle que}\ g_{\theta,\gamma}(T)e_\theta\zeta_d=e_\theta\alpha_\gamma(\mathrm{Col}(\eta_d))$$

Bien entendu si θ est non trivial $g_{\theta,\gamma}(T)\in\mathbb{Z}_p[\theta][[T]]$. On voit aussi facilement que si θ est impair alors $g_{\theta,\gamma}(T)=0$. Tsuji démontre alors le théorème

Théorème 3.17 ([Tsu99] theorem 4.3) *Pour tout θ pair on a*

$$g_{\theta,\gamma}((\kappa(\gamma))^s-1)=L_p(1-s,\theta).$$

Pour expliciter le lien avec les séries d'Iwasawa $f(T,\theta)$ il suffit de rappeler l'identité $L_p(1-s,\theta)=f((1+dp)^{1-s}-1,\theta)$ du théorème 3.12. On en déduit immédiatement le corollaire :

Corollaire 3.18 *Choisissons γ tel que $\kappa(\gamma)=(1+dp)\in\mathbb{Z}_p^\times$. Alors on a*

$$f(T,\theta)=g_{\theta,\gamma}((1+dp)(T+1)^{-1}-1),$$

et réciproquement

$$g_{\theta,\gamma}(T)=f((1+dp)(T+1)^{-1}-1,\theta).$$

De cette façon, on a retrouvé la collection des fonctions L_p à partir de la collection des suites cohérentes en normes d'unités cyclotomiques. Pour cette raison on doit vraiment comprendre les unités cyclotomiques comme des incarnations algébriques des fonctions L. Ce point de vue motive évidemment l'étude de ces unités pour elles-mêmes. Il rend aussi nettement plus naturel les formules analytiques comme celle du corollaire 2.4 et du théorème 3.9. Ces formules trouvent leur explication ultime avec la Conjecture Principale qui affirme que les séries précédentes engendrent les idéaux caractéristiques ($\mathrm{car}(M)$) du §3.1 associés aux modules M provenant au niveau fini des invariants algébriques fondamentaux de l'arithmétique (essentiellement des variations sur le groupe des classes d'idéaux).

3.3 Conjecture Principale.

Les principaux objets algébriques étudiés dans l'arithmétique des corps globaux sont des variations sur les unités d'une part et sur les groupes de classes d'idéaux d'autre part. Ces deux types d'objets ont toujours été naturellement reliés. Mentionnons par exemple les formules d'ordre provenant de l'analyse, comme la formule analytique du nombre de classes, et les suites exactes issues de la théorie du corps de classes. Le lien ultime est établi dans la Conjecture Principale qui affirme "l'égalité" entre les séries caractéristiques, d'une part de certains groupes de classes d'unités, et d'autre part de certains groupes des classes d'idéaux. De plus un générateur de cette série caractéristique commune s'explicite à l'aide des séries $f(T,\theta)$ ou $g_{\theta,\gamma}(T)$ du paragraphe 3.2.

3.3.1 Modules Standard.

On rappelle ici les notations classiques de la théorie d'Iwasawa cyclotomique, dont certaines ont déjà été utilisées précédemment. La lettre K désigne un corps de nombres, et $p \neq 2$ est le nombre premier fixé depuis le début du §2.5.

- Pour tout groupe abélien A, on note $\overline{A}$ la p-completion de A, i.e. la limite projective $\overline{A} = \lim A/A^{p^n}$. Si A est de type fini sur $\mathbb{Z}$, alors $\bar{A} \cong A \otimes \mathbb{Z}_p$.
- U_K désigne le groupe des unités de K.
- U'_K désigne le groupe des (p)-unités de K, c'est-à-dire les éléments de $F^\times$ de valuation triviale en toute place finie v ne divisant pas p.
- $\mathcal{N}_K$ est le groupe multiplicatif des nombres semi-locaux. Comme module sur $\mathbb{Z}_p$, $\mathcal{N}_K = \prod_{v|p} \overline{K_v^\times}$ où K_v est le complété de K en la place

v.

- $\mathcal{U}_K$ est le groupe multiplicatif des unités semi-locales de K. Comme module sur $\mathbb{Z}_p$, $\mathcal{U}_K = \prod_{v|p} U_v^1$ où U_v^1 est le groupe des unités principales de K_v, c'est-à-dire les unités $\equiv 1$ modulo l'idéal maximal de K_v.
- $\mathfrak{X}_K$ est le groupe de Galois sur K de la pro-p-extension abélienne (p)-ramifiée (c'est-à-dire non ramifiée en toute place ne divisant pas p) maximale de K.
- X'_K désigne la p-partie de $\mathrm{Cl}'(K)$ qui lui même est le quotient de $\mathrm{Cl}(K)$ par le sous-groupe engendré par les classes des idéaux premiers divisant p.
- X_K désigne la p-partie de $\mathrm{Cl}(K)$ le groupe des classes d'idéaux de K.

La conjecture de Leopoldt prédit que l'application basique $\overline{U}_K \longrightarrow \mathcal{U}_K$ est injective. Lorsque F est abélien sur $\mathbb{Q}$ la conjecture de Leopoldt pour F est démontrée : Ax dans [Ax65] réduit cette conjecture pour les corps abéliens à l'analogue p-adique du théorème de Baker, et Brumer a démontré cet analogue dans [Bru67]. Lorsque K est galoisien sur $\mathbb{Q}$, de groupe $G(K/\mathbb{Q})$, les modules semi-locaux $\mathcal{U}_K$ et $\mathcal{N}_K$ sont munis de l'action induite à $G(K/\mathbb{Q})$ définie par l'isomorphisme

$$\mathcal{N}_K \cong \overline{K_v^\times} \otimes_{\mathbb{Z}_p[G(K_v/\mathbb{Q}_p)]} \mathbb{Z}_p[G(K/\mathbb{Q})].$$

Considérons maintenant la $\mathbb{Z}_p$-extension cyclotomique F_∞/F d'un corps abélien F, et notons F_n l'unique sous corps de F_∞ tel que $[F_n : F] = p^n$. On va noter par $\overline{C}_n$ le pro-p-complété des unités circulaires de F_n. On indique par un indice $_n$ les modules arithmétiques relatifs à F_n. On indique la limite projective de ces objets (pour les applications de normes) par un indice $_\infty$. Cela définit les notations $\mathcal{U}_n$, $\overline{U}_n$, ... et $\mathcal{U}_\infty$, $\overline{U}_\infty$ etc... L'étude du groupe de classes $\mathrm{Cl}(F)$ puis de son analogue au niveau infini X_∞ furent les premières motivations de la théorie d'Iwasawa. À l'usage il devenu clair que le module $\mathfrak{X}_\infty$ (ou plutôt sa Λ-torsion) est plus pertinent en théorie d'Iwasawa. La conjecture de Leopoldt (démontrée ici puisque F est abélien) pour F et p est équivalente à l'égalité $\mathrm{rang}_{\mathbb{Z}_p}(\mathfrak{X}_\infty)_\Gamma = r_2$ où r_2 désigne le nombre de plongements complexes de F. Je vais maintenant rappeler trois formulations classiques (et équivalentes) de la Conjecture Principale.

3.3.2 Les formulations totalement réelles.

On suppose dans cette sous-section que F est totalement réel. Pour simplifier la suite de l'exposé on suppose en outre que p est (au plus) modérément ramifié dans $F/\mathbb{Q}$. Je rappelle maintenant l'une des suites exactes issues de la théorie du corps de classes et qui décrit (en partie) $\mathfrak{X}_\infty$. Il s'agit de la suite

de ramification :

$$(R) \qquad 0 \longrightarrow \overline{U}_\infty \longrightarrow \mathcal{U}_\infty \longrightarrow \mathfrak{X}_\infty \longrightarrow X_\infty \longrightarrow 0\,.$$

En prenant le quotient par $\overline{C}_\infty$ on obtient :

$$(R') \qquad 0 \longrightarrow \overline{U}_\infty/\overline{C}_\infty \longrightarrow \mathcal{U}_\infty/\overline{C}_\infty \longrightarrow \mathfrak{X}_\infty \longrightarrow X_\infty \longrightarrow 0\,.$$

Il est bien connu que chacun des quatres Λ-modules intervenant dans cette suite est de type fini et de torsion. En outre les invariants μ de ces modules sont triviaux, même si ce fait est un peu moins connu des non-spécialistes. Pour le module $\overline{U}_\infty/\overline{C}_\infty$ une démonstration (comprenant $p = 2$) est donnée par Greither dans [FG04]. Je donne une autre démonstration et un aperçu concernant les trois autres modules dans [Bel05]. Soit $\theta\colon G(F/\mathbb{Q}) \longrightarrow \overline{\mathbb{Q}}^\times$ un caractère de Dirichlet non trivial. Puisque les invariants μ concernés sont triviaux, en appliquant à $(R)'$ n'importe quel foncteur (raisonnable[2]) de θ-composante $M \rightsquigarrow M(\theta)$, on obtient un complexe pseudo-exact (i.e. à groupes de cohomologie finis) :

$$(R'(\theta)) \quad 0 \longrightarrow \overline{U}_\infty/\overline{C}_\infty(\theta) \longrightarrow \mathcal{U}_\infty/\overline{C}_\infty(\theta) \longrightarrow \mathfrak{X}_\infty(\theta) \longrightarrow X_\infty(\theta) \longrightarrow 0\,.$$

De par sa construction même, la série $g_{\theta,\gamma}(T)$ engendre l'idéal caractéristique sur $\mathbb{Z}_p[\theta][[T]]$ de $\overline{U}_\infty/\overline{C}_\infty(\theta)$. En effet, en partant de la suite exacte du théorème 3.15 on obtient un complexe pseudo-exact :

$$0 \longrightarrow \mathrm{Ind}_{\mathfrak{P}}(\mathbb{Z}_p(1))(\theta) \longrightarrow \frac{\mathcal{U}_\infty(\theta)}{\overline{C}_\infty(\theta)} \xrightarrow{\theta(\mathrm{Col})} \frac{\mathbb{Z}_p[\theta][[T]]}{(g_{\theta,\gamma}(T))} \xrightarrow{\kappa} \mathrm{Ind}_{\mathfrak{P}}(\mathbb{Z}_p(1))(\theta) \longrightarrow 0\,.$$

La Conjecture Principale de la théorie d'Iwasawa (dans ce cadre c'est le théorème de Mazur-Wiles [MW84]) affirme l'égalité :

Théorème 3.19

$$(\mathrm{car}(\mathfrak{X}_\infty(\theta))) = (g_{\theta,\gamma}(T)).$$

Cette formulation de la conjecture principale est, à mon avis, à la fois la plus parlante et la plus simple. Par la construction du §3.2.3 cette conjecture est équivalente à l'égalité

$$(\mathrm{car}(\mathfrak{X}_\infty(\theta))) = (\mathrm{car}(\mathcal{U}_\infty/\overline{C}_\infty(\theta))).$$

Par le complexe $(R'(\theta))$ la conjecture principale est aussi équivalente à l'égalité

$$(\mathrm{car}(X_\infty(\theta))) = (\mathrm{car}(\overline{U}_\infty/\overline{C}_\infty(\theta))).$$

C'est cette dernière égalité qui se démontre avec le système d'Euler cyclotomique (voir l'appendice de Rubin dans [Lan90] et la démonstration générale incluant $p = 2$ dans [Gre92]).

[2]Par exemple les θ-parties et θ-quotients.

3.3.3 Dualité de Kummer.

Pour pouvoir utiliser la dualité de Kummer on suppose dans cette sous-section que ζ_p appartient à F. Pour simplifier l'exposé, on suppose en outre que $F = K(\zeta_p)$ pour un corps K abélien totalement réel non ramifié en p. On peut donc identifier $\mathrm{Gal}(F/\mathbb{Q})$ au produit direct $\mathrm{Gal}(F/\mathbb{Q}) = \Delta \times G_0$, avec $G_0 = \mathrm{Gal}(F/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Soit τ la conjugaison complexe dans $\mathrm{Gal}(F/\mathbb{Q})$. L'hypothèse K totalement réel est équivalente à $\tau \in G_0$. Pour tout $i \in \mathbb{Z}$ on note e_i l'idempotent de $\mathbb{Z}_p[G_0]$ associé à la i-ième puissance du caractère de Teichmüller ω^i. On note $A_\infty = \varinjlim X_n$ la limite inductive (pour les morphismes d'extension des idéaux) des p-groupes de classes des F_n. Soit $V \subset \varinjlim(F_n \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ le radical de Kummer de $\mathfrak{X}_\infty$, et $E_\infty = \varinjlim U_n$ la limite inductive des unités des F_n. On a une suite exacte :

$$0 \longrightarrow E_\infty \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow V \longrightarrow A_\infty \longrightarrow 0\ .$$

Lorsque i est impair, puisque $\tau \in G_0$, l'involution τ agit simultanément trivialement et par -1 sur E_∞. En particulier pour tout i impair on a un isomorphisme de modules galoisiens $e_i V \cong e_i A_\infty$. Pour tout $\mathbb{Z}_p$-module galoisien M et tout entier $k \in \mathbb{Z}$ on note $M(k) = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)^{\otimes k}$ le k-ième twist de Tate. On obtient l'isomorphisme (galoisien) :

Proposition 3.20 ([Was97] proposition 13.32) *On munit le $\mathbb{Z}_p$-module $\mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ de l'action de Galois $(gf)(x) := f(g^{-1}x)$. Soit j un entier pair. Alors*

$$e_j\mathfrak{X}_\infty(-1) \cong \mathrm{Hom}_{\mathbb{Z}_p}(e_{1-j}A_\infty, \mathbb{Q}_p/\mathbb{Z}_p).$$

Soit θ un caractère pair de F. Alors θ peut s'écrire $\theta = \omega^j\varphi$ avec $\varphi \in \widehat{\Delta}$. Comme Δ commute avec $G_0 \times \Gamma$ tout foncteur (raisonnable) $M \rightsquigarrow M(\varphi)$ de φ-composante va commuter avec le twist de Tate. Il suit un isomorphisme $e_j\mathfrak{X}_\infty(\varphi)(-1) \cong \mathrm{Hom}_{\mathbb{Z}_p}(e_{1-j}A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)(\varphi)$. De sorte que si $F(T)$ est une série caractéristique de $\mathfrak{X}_\infty(\theta)$ avec $\theta = \omega^j\varphi$ alors $F(\kappa(\gamma)(1+T)-1)$ est une série caractéristique de $\mathrm{Hom}_{\mathbb{Z}_p}(e_{1-j}A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)(\varphi)$. Soit d le conducteur de φ. Reprenons le générateur γ de Γ vérifiant $\kappa(\gamma) = 1 + dp$. En observant l'égalité $g_{\theta,\gamma}((1+dp)(1+T)-1) = f((1+T)^{-1}-1, \theta)$ on obtient la seconde formulation équivalente de la Conjecture Principale :

Théorème 3.21 *Soit φ un caractère de Dirichlet pair tel que $\varphi(p) \neq 0$. Alors pour tout entier j pair on a l'égalité entre idéaux de $\mathbb{Z}_p[\varphi][[T]]$:*

$$\mathrm{car}(\mathrm{Hom}_{\mathbb{Z}_p}(e_{1-j}A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)(\varphi)) = (f((1+T)^{-1}-1, \omega^j\varphi))$$

3.3.4 Retour aux classes d'idéaux.

En utilisant la théorie des modules adjoints d'Iwasawa on démontre que $\mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ est pseudo-isomorphe au module $\widetilde{X}_\infty$ défini à partir de X_∞ en inversant l'action de Γ (voir par exemple [Was97] proposition 15.34). Cependant on doit ici en outre se préoccuper de l'action de Δ.

Remarque technique : Pour fixer les idées et suivre cette action dans les constructions de l'adjoint §15.5 de [Was97] il semble plus facile d'utiliser les foncteurs φ-partie $M \rightsquigarrow M^\varphi$ (exact à gauche) et φ-quotient $M \rightsquigarrow M_\varphi$ (exact à droite) ; voir par exemple [Tsu99] et [Belt] pour les définitions et propriétés basiques. A l'arrivée, puisque les invariants μ concernés sont triviaux, toutes ces différentes φ-composantes sont pseudo-isomorphes.

On a des pseudo-isomorphismes

$$\mathrm{Hom}_{\mathbb{Z}_p}(e_{1-j}A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)_\varphi \sim \mathrm{Hom}_{\mathbb{Z}_p}(e_{1-j}A_\infty^{\varphi^{-1}}, \mathbb{Q}_p/\mathbb{Z}_p) \sim \widetilde{e_{1-j}X_\infty^{\varphi^{-1}}}.$$

On obtient ainsi la troisième formulation équivalente de la Conjecture Principale :

Théorème 3.22 *Soit φ un caractère de Dirichlet pair tel que $\varphi(p) \neq 0$. Alors pour tout entier j pair on a l'égalité entre idéaux de $\mathbb{Z}_p[\varphi][[T]]$:*

$$\mathrm{car}(X_\infty^{\omega^{1-j}\varphi^{-1}})) = (f(T, \omega^j\varphi)).$$

C'est essentiellement cet énoncé qui est démontré dans [MW84] (modulo la trivialité de l'invariant μ). Ce théorème ne donne aucune information sur les classes réelles puisque le caractère $\omega^{1-j}\varphi^{-1}$ est impair. Pour un caractère θ pair le pendant analytique $L_p(s, \omega\theta^{-1})$ est identiquement nul. La conjecture de Greenberg prédit que X_∞^+ est fini autrement dit que l'on peut prendre $f(T, \omega\theta - 1) = 1$ dans l'énoncé de 3.22 pour les caractères φ impairs. Cette conjecture a été vérifiée par une multitude de calculs numériques. Elle est aussi équivalente à la finitude de $\overline{U}_\infty/\overline{C}_\infty$. En particulier si l'on reprend la suite exacte (R') du §3.3.2 on constate que la conjecture de Greenberg entraîne immédiatement la formulation totalement réelle de la Conjecture Principale. Compte-tenu de la technicité des preuves actuelles de la Conjecture Principale, cela laisse peu d'espoir pour une démonstration simple de la conjecture de Greenberg.

Chapitre 4

Une question de Kolster.

Dans ce chapitre F désigne un corps de nombres abélien réel, et $p \neq 2$ un nombre premier fixé. On va étudier l'arithmétique de la $\mathbb{Z}_p$-extension F_∞/F de F.

4.1 Washington contre Sinnott.

Définition 4.1 *Soit K un corps abélien de conducteur n. Rappelons que $C_{\mathbb{Q}(\zeta_n)}$ (définition 2.1) désigne le module des unités circulaires à la Sinnott de $\mathbb{Q}(\zeta_n)$. On appelle unités cyclotomiques de Washington de K et l'on note* Was_K *le module*

$$\mathrm{Was}_K = C_{\mathbb{Q}(\zeta_n)} \bigcap K.$$

La terminologie "unités de Washington" apparaît à ma connaissance pour la première fois dans [KN95], où il est fait référence à la première page du chapitre 8 de [Was97]. Bien entendu dans la suite on notera $\mathrm{Was}_n = \mathrm{Was}_{F_n}$ et $\overline{\mathrm{Was}}_\infty = \varprojlim \overline{\mathrm{Was}}_n$ la limite projective des pro-p-complétés $\overline{\mathrm{Was}}_n$. On a trivialement l'inclusion $C_K \subset \mathrm{Was}_K$. D'autre part le module des unités de Washington satisfait la "propriété de descente" $\mathrm{Was}_L \cap K = \mathrm{Was}_K$ pour toute extension L/K (par définition on se ramène au cas particulier L et K cyclotomique ; puis c'est un théorème de Gold et Kim [GK89]). Pour le module de Sinnott on dispose de contre-exemples à la propriété de descente (voir [Gre93]). En particulier l'inclusion $C_K \subset \mathrm{Was}_K$ est stricte en général. Cependant la question (attribuée à Kolster dans [KN95]) de l'égalité entre $\overline{C}_\infty$ et $\overline{\mathrm{Was}}_\infty$ se posait encore jusqu'a récemment. Dans l'article [KN95] Kučera et Nekovar montrent que l'indice $(\overline{\mathrm{Was}}_\infty : \overline{C}_\infty)$ est fini (en majorant uniformément avec n les indices $(\overline{\mathrm{Was}}_n : \overline{C}_n)$ mais échouent à démontrer l'égalité $\overline{C}_\infty = \overline{\mathrm{Was}}_\infty$. En fait, cette égalité n'a pas lieu en général : j'ai donné des

contre-exemples dans [Bel02] et Kučera en a trouvé indépendamment et simultanément d'autres (voir [Kuč03]), ce qui clôt cette question. Cette question, à mon avis depuis sa motivation même, est liée à la $G_n = \mathrm{Gal}(F_n/F)$-structure des $\overline{C}_n$ c'est-à-dire à la Λ-liberté de $\overline{C}_\infty$. Pendant et après ma thèse j'ai essayé d'établir en toute généralité cette Λ-liberté jusqu'à trouver des contre-exemples et démontrer l'équivalence entre la Λ-liberté de $\overline{C}_\infty$ et l'égalité $\overline{\mathrm{Was}}_\infty = \overline{C}_\infty$ dans [Bel02].

4.2 G_n-Structure des unités circulaires.

Avant d'arriver à décrire la structure de Λ-module de $\overline{C}_\infty$ j'ai étudié dans ma thèse ([Bel98],[Bel97]) la $\mathbb{Z}_p[G_n]$-structure de $\overline{C}_n$. Pour ces travaux, j'ai supposé que p ne se ramifie pas dans $F/\mathbb{Q}$.

J'ai défini par des générateurs explicites un module galoisien noté $\mathcal{D}_n(F)$ qui contient les unités cyclotomiques "nouvelles" de F_n en ce sens que l'intersection $\mathcal{D}_n(F) \cap C_n$ et le sous-groupe C_0 engendrent $\overline{C}_n$ sur $\mathbb{Z}_p$. J'ai aussi démontré que le module explicite $\mathcal{D}_n(F)$ contient toutes les "normes universelles" d'unités cyclotomiques (en particulier $\overline{C}_\infty \subset \varprojlim_n \mathcal{D}_n(F)$, avec un co-noyau évident).

J'ai mis en évidence deux hypothèses techniques mais naturelles (appelées hypothèse A et B, dans le texte) l'hypothèse B étant le p-adifié de l'hypothèse A. Sous l'hypothèse A j'ai décrit explicitement la $\mathbb{Z}[G_n]$-structure de $\mathcal{D}(K)$, et respectivement la $\mathbb{Z}_p[G_n]$-structure de $\mathcal{D}_n(K) \otimes \mathbb{Z}_p$ sous l'hypothèse B ([Bel97] théorème 4.5). Dans les deux cas, on trouve la somme directe d'un facteur libre avec une puissance de l'idéal d'augmentation. Le rang de chaque facteur s'exprime très simplement à partir de la décomposition de p dans F.

J'ai aussi démontré que les hypothèses ci-dessus sont vérifiées dans de nombreux cas particuliers intéressants. Par exemple l'hypothèse A qui entraîne l'hypothèse B est réalisée lorsque le groupe de Galois de $K/\mathbb{Q}$ est cyclique ou bien lorsque K est un corps de genre à la Fröhlich. En conséquence l'hypothèse B est vraie pour $p \neq 2$ lorsque K est le sous-corps réel maximal d'un corps cyclotomique. Je décris aussi deux exemples de corps qui ne satisfont ni l'hypothèse ni la conclusion du théorème 4.5 de [Bel97].

Par un passage à la limite projective évident on déduit du théorème 4.5 de [Bel97] la Λ-liberté de $\overline{C}_\infty$ sous l'hypothèse B. La situation générale n'était pourtant toujours pas claire. Cela a fournit (beaucoup) d'exemples pour lesquels la réponse à la question de Kolster est positive, et à ce stade de mes recherches je croyais encore possible de démontrer la Λ-liberté de $\overline{C}_\infty$ en toute généralité.

4.3 Sous-modules d'Unités.

L'objet de l'article [Bel02] est de dégager une condition nécessaire et suffisante à la liberté du Λ-module $\overline{C}_\infty$. La proposition 4.2 fournit un critère suffisamment fin pour conduire à une équivalence si on l'applique au module $\overline{C}_\infty$. Cette équivalence (théorème 4.4) est le résultat principal de [Bel02]. Ensuite j'illustre le théorème 4.4 par des contre-exemples à la Λ-liberté de $\overline{C}_\infty$. Je donne une famille infinie d'exemples pour lesquels on démontre que cette liberté n'a pas lieu. D'autres exemples avec la même propriété ont été étudiés indépendamment par R. Kučera ([Kuč03]) dans le but d'établir la différence entre les modules $\overline{C}_\infty$ et $\overline{\mathrm{Was}}_\infty$. En cours de route j'établis aussi que ces modules sont égaux si et seulement si $\overline{C}_\infty$ est Λ-libre (proposition 4.6).

4.3.1 Critère de Λ-liberté des unités circulaires.

On détaille le contexte général dans lequel le critère de la descente galoisienne s'applique, contexte qui se produit très souvent en arithmétique. Il s'agit de la donnée de deux suites, disons $M_n \subset L_n$, de $\mathbb{Z}_p[G_n]$-modules munis, pour $m \geq n$, d'homomorphismes équivariants de *norme* $N_{m,n}\colon L_m \longrightarrow L_n$ et d'*extension* $i_{n,m}\colon L_n \longrightarrow L_m$ tels que :

1) Les restrictions des $N_{n,m}$ et des $i_{m,n}$ définissent des homomorphismes $N_{m,n}\colon M_m \longrightarrow M_n$ et $i_{n,m}\colon M_n \longrightarrow M_m$
2) les composés $i_{n,m} \circ N_{m,n}$ coïncident avec la multiplication par la *trace algébrique* $\mathrm{Tr}_{m,n} := \sum_{g \in \mathrm{Gal}(K_m/K_n)} g \in \mathbb{Z}_p[G_m]$.
3) les composés $N_{m,n} \circ i_{n,m}$ coïncident avec la multiplication par p^{m-n}.

Dans ce contexte on a le critère :

Proposition 4.2 ([Bel02] proposition 1.3) *On suppose que les suites L_n et M_n vérifient les conditions suivantes :*

1. $L_\infty := \varprojlim L_n$ *est Λ-libre.*
2. *Les homomorphismes $i_{n,m}\colon L_n \longrightarrow L_m^{\mathrm{Gal}(F_m/F_n)}$ sont injectifs.*
3. *La suite M_n vérifie asymptotiquement la* "descente galoisienne"*, (i.e. il existe un $N \in \mathbb{N}$ tel que pour tout $n \geq N$ on l'égalité $M_{n+1}^{\mathrm{Gal}(F_{n+1}/F_n)} = i_{n,n+1}(M_n)$).*

Alors $M_\infty := \varprojlim M_n$ est aussi Λ-libre.

Par le théorème 7.2 de [Kuz72] le module $\overline{U}'_\infty$ est Λ-libre (ici de rang $[F : \mathbb{Q}]$). Ce résultat a été redémontré dans [KNF96] et une troisième preuve plus simple mais s'appuyant sur la conjecture de Leopoldt (valide ici car F est

abélien) est donnée dans [Bel05]. Le module $L_\infty = \overline{U}'_\infty$ satisfait donc aux conditions 1. et 2. de la proposition 4.2. Puisque la suite $M_n = \overline{\mathrm{Was}}_n$ satisfait à la troisième et dernière condition de 4.2, cela démontre le corollaire :

Corollaire 4.3 $\overline{\mathrm{Was}}_\infty$ *est* Λ*-libre (de rang* $[F : \mathbb{Q}]$*).*

Par contre si l'on prend pour $M_\infty = \overline{C}_\infty$ on obtient alors une équivalence.

Théorème 4.4 ([Bel02] théorème 2.2) *Le* Λ*-module* $\overline{C}_\infty$ *est libre si et seulement si la suite* $M_n = \overline{C}_n$ *vérifie la condition 3 de 4.2, à savoir :*

$$\overline{C}_\infty \text{ est } \Lambda \text{ libre} \iff \exists\, N \in \mathbb{N},\, \forall n \geq N,\, \overline{C}_{n+1}^{\mathrm{Gal}(K_{n+1}/K_n)} = i_{n,n+1}(\overline{C}_n) \cong \overline{C}_n.$$

Pour démontrer ce théorème j'utilise un "lemme-clé" qui est essentiellement une conséquence des relations de distribution du §2.2.

Lemme 4.5 ([Bel02] lemme 2.5) *Soit* $n \in \mathbb{N}$ *et soit* I_n *le corps d'inertie en* p *de* K_n *(i.e. le plus grand sous-corps de* K_n *dans lequel* p *ne se ramifie pas). On note* $\widetilde{C}_n$ *les "normes universelles d'unités circulaires" c'est-à-dire l'image du morphisme naturel* $\overline{C}_\infty \longrightarrow \overline{C}_n$*. Alors on a*

$$\overline{C}_n = \overline{C}_{I_n}\, \widetilde{C}_n.$$

La suite de corps I_n *est manifestement stationnaire et si* I *désigne le corps d'inertie de* p *dans* K_∞*, on a l'égalité pour tout* n *tel que* $I \subset K_n$ *:*

$$\overline{C}_n = \overline{C}_I\, \widetilde{C}_n$$

Le corollaire 4.3 en conjonction avec le théorème de Kučera et Nekovar sur la finitude de $(\overline{\mathrm{Was}}_\infty : \overline{C}_\infty)$ permet de reformuler la question de Kolster :

Proposition 4.6 ([Bel02] proposition 3.6) $\overline{C}_\infty$ *est* Λ*-libre si et seulement si* $\overline{C}_\infty = \overline{\mathrm{Was}}_\infty$*.*

4.3.2 Contre-exemples.

A partir du théorème 4.4 qui donne une équivalence, il est naturel de se demander si les deux alternatives peuvent effectivement se produire. On connaît de nombreux exemples de corps F pour lesquels $\overline{C}_\infty$ est Λ-libre. Je reviens là-dessus en section 4.4. Cependant on a vu que les unités circulaires à la Sinnott ne vérifient pas toujours la "descente galoisienne". En particulier 4.4 n' entraîne pas la liberté de $\overline{C}_\infty$. Je présente une liste d'exemples de corps F pour lesquels cette liberté n'a pas lieu. Pour produire ces contre-exemples on va utiliser des hypothèses de décomposition assez contraignantes dans le

style de [Gre93]. Ces hypothèses permettent de mieux contrôler la structure galoisienne des unités circulaires et simplifient notablement les calculs qui suivent. Ce fait justifie la terminologie *"günstige* $(p+1)$*-tuple"* de [Gre93]. Énonçons ces conditions. A partir d'ici, et jusquà la fin de cette sous-section, on suppose que le corps de nombres abélien F et le nombre premier p vérifient les trois conditions suivantes :

1– le conducteur de F est le produit sans facteurs carrés $f_F = \prod_{i=1}^{i=p+1} l_i$ de $p+1$ nombres premiers l_i tels que $l_i \equiv 1[p]$ et pour chaque $j \neq i$ il existe un entier $x_{i,j}$ tel que $l_i \equiv x_{i,j}^p[l_j]$.

2– $G := \mathrm{Gal}(F/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^2$

3– Notons $F^1, F^2, \ldots, F^{p+1}$ les $(p+1)$ sous-corps non triviaux de F. On suppose en outre que quitte à renuméroter ces sous-corps, leur conducteur vaut :

$$\mathrm{cond}(F^j) = \prod_{i=1, i\neq j}^{i=p+1} l_i$$

Remarque :

- En reprenant le raisonnement de [Gre93] qui s'appuie sur le théorème de densité de Čebotarev, on peut démontrer l'existence (d'une infinité) de $(p+1)$-uples de premier $(l_i)_{i=1}^{p+1}$ tels que p et tout sous-corps de $\mathbb{Q}(\zeta_{\prod l_i})$ vérifie la condition 1. Ce sont de tels $(p+1)$-uples qui furent dénommés *günstige* $(p+1)$*-tuple* dans [Gre93].
- Ensuite étant fixé un tel günstige $(p+1)$-uple $l_1, \ldots, l_{p+1}$ on peut vérifier que $\mathbb{Q}(\zeta_{\prod l_i})$ contient un sous-corps F vérifiant 2- et 3- : c'est un exercice sur les groupes abéliens laissé au lecteurs.
- Alternativement l'exemple du §IV.2 de [Bel98] vérifie les conditions ci-dessus pour $p = 3$.

Théorème 4.7 ([Bel02] théorème 3.1) *Si F vérifient les hypothèses 1– à 3– alors $\overline{C}_\infty$ n'est pas Λ-libre.*

4.4 Des exemples de liberté de $\overline{C}_\infty$.

Lorsque le corps F est le sous-corps réel maximal d'un corps cyclotomique, on sait par des résultats sur les distributions à la Kubert-Lang que $\overline{C}_\infty$ est Λ-libre (voir par exemple [Kuz96]). Plus généralement, par un passage à la limite immédiat, on peut déduire de [Bel98] une condition suffisante et des exemples supplémentaires où $\overline{C}_\infty$ est Λ-libre avec p non ramifié dans F. Dans l'appendice à [LMN] j'ai formulé une condition (appelée (gHB)) indépendante de la ramification de p dans F et qui entraîne la Λ-liberté de $\overline{C}_\infty$. De plus, tous les exemples connus de corps F tels que $\overline{C}_\infty$ soit libre sur Λ satisfont

à la condition (gHB). Il n'y a pas d'autre raison de penser qu'il y ait une équivalence (et personnellement j'en doute).

Lemme 4.8 ([LMN] lemma 6.1) *Soit $L \subset F_\infty$ le sous-corps maximal de F_∞ tel que p soit (au plus) modérément ramifié dans L. On note L_∞/L sa $\mathbb{Z}_p$-extension cyclotomique, on pose $\Lambda_L := \mathbb{Z}_p[[\mathrm{Gal}(L_\infty/L)]]$. On a :*

1. *$\overline{C}_\infty$ dépend seulement de F_∞ et pas de F.*
2. *$L_\infty = F_\infty$.*
3. *$\overline{C}_\infty$ est Λ-libre si et seulement si $\overline{C}_\infty$ est Λ_L-libre.*

On utilise quelques notations supplémentaires. Elles sont proches de celles utilisées dans [Bel98] mais pas formellement identiques. Soit $\mathcal{P}$ l'ensemble des premiers rationnels $l \neq p$ qui sont ramifiés dans $F/\mathbb{Q}$. Le cas $\mathcal{P} = \emptyset$ est trivial mais autorisé. Pour tout nombre supernaturel s on pose $\mathbb{Q}(s) = \mathbb{Q}(\zeta_s)$. Pour tout $J \subset \mathcal{P}$ et tout $n \in \mathbb{N} \cup \{\infty\}$, on pose $F_n(J) := \mathbb{Q}(\prod_{l \in J} l^\infty p^\infty) \cap F_n$. On notera $F(J) := F_0(J)$, $G(J) = \mathrm{Gal}(F_\infty(J)/\mathbb{B}_\infty)$, et $G = G(\mathcal{P})$. Pour tout corps de nombres abélien K on écrit $\mathrm{cond}(K)$ pour son conducteur. Pour chaque $n \in \mathbb{N}$ et tout $J \subset \mathcal{P}$ on note $\varepsilon_n(J)$ le nombre cyclotomique suivant (c'est une unité si $J \neq \emptyset$) :

$$\varepsilon_n(J) := N_{\mathbb{Q}(\mathrm{cond}(F_n(J)))/F_n(J)}(1 - \zeta_{\mathrm{cond}(F_n(J))}).$$

Les $\varepsilon_n(J)$ forment une suite cohérente en norme. De sorte qu'en fixant un γ engendrant $\mathrm{Gal}(\mathbb{B}_\infty/\mathbb{Q})$ on peut définir $\varepsilon_\infty(J) \in \overline{C}_\infty$ par la formule :

$$\varepsilon_\infty(J) := \begin{cases} (\varepsilon_n(J))_{n\in\mathbb{N}} \text{ if } J \neq \emptyset \\ (\varepsilon_n(\emptyset)^{(\gamma-1)})_{n\in\mathbb{N}} \text{ else.} \end{cases}$$

Cela permet de formuler un lemme utile (c'est un variante du lemme 2.3 de [Gre92]).

Lemme 4.9 ([LMN] lemma 6.2) *Le système $\{\varepsilon_\infty(J), J \subset \mathcal{P}\}$ engendre $\overline{C}_\infty$ sur $\Lambda_L[G]$.*

Bien sûr ces générateurs ne sont pas linéairement indépendants. Ils vérifient les relations déduites par passage à la limite à partir des relations de distribution. C'est pour mieux contrôler ces relations que j'utilise l'hypothèse (gHB) que j'énonce ci-dessous :

Définition 4.10 *Pour tout $J \subset \mathcal{P}$ on appelle l'idéal de norme associé à J on note $N(J)$ l'idéal de $\mathbb{Z}_p[G(J)]$ engendré par les traces*

$$N(J) := \left\langle T_{F_\infty(J)/F_\infty(J-\{l\})};\, l \in J \right\rangle.$$

On dit que le couple (F, p) vérifie l'hypothèse B généralisée (en abrégé (gHB)) si et seulement si pour tout $J \subset \mathcal{P}$ le quotient $\mathbb{Z}_p[G(J)]/N(J)$ est sans torsion.

Cette hypothèse est plutôt technique mais parfaitement naturelle vis-à-vis de la preuve de 4.12. La proposition qui suit donne une multitude d'exemples de corps vérifiant (gHB).

Proposition 4.11 ([LMN] proposition 6.5) *Pour tout $l \in \mathcal{P}$ on note $I_l \subset G$ le sous-groupe d'inertie pour l relativement à l'extension $F_\infty/\mathbb{B}_\infty$. L'une quelconque des conditions ci-dessous entraîne que le couple (F,p) satisfait à (gHB) :*

1. *Les $\overline{I}_l$, $l \in \mathcal{P}$ sont facteurs directs les uns des autres. Autrement dit le morphisme naturel $\bigoplus_{l\in\mathcal{P}} \overline{I}_l \longrightarrow \overline{G}$ est injectif.*
2. $\dim_{\mathbb{F}_p}(G/pG) \leq 1$, *ou de façon équivalente $\overline{G}$ est cyclique.*
3. $\#\mathcal{P} \leq 2$

Le résultat principal de l'appendice à [LMN] est le théorème suivant :

Théorème 4.12 ([LMN] theorem 6.6) *On suppose que le couple (F,p) vérifie la condition (gHB). Alors $\overline{C}_\infty$ est Λ_L-libre de rang $[L:\mathbb{Q}]$ et Λ-libre de rang $[F:\mathbb{Q}]$.*

En corollaire, la question de Kolster admet une réponse positive dès que le couple (F,p) vérifie (gHB). Il me semble que la condition (gHB) est optimale. En effet cette condition permet de réunir en une seule démonstration tous les exemples où la Λ-liberté de $\overline{C}_\infty$ était connue auparavant par des méthodes plus ou moins sophistiquées. Mais aussi, avec la proposition 4.11, on obtient une très large classes d'exemples nouveaux de corps abéliens F pour lesquels $\overline{C}_\infty$ est libre. Par exemple tout corps abélien F tel que $X_F = 0$ vérifie la condition 1 de la proposition 4.11.

Chapitre 5

Classes d'idéaux et classes d'unités.

5.1 Formules d'indice raffinées.

Le résultat principal de l'article [BN01] (théorème 5.4) est un raffinement de la formule de Sinnott (Théorème 2.6), qui est p-adique ($p \neq 2$) et "caractère par caractère". La formule p-adique sans caractère est facile à obtenir : il suffit de tensoriser par $\mathbb{Z}_p$ les réseaux qui interviennent dans la formule de Sinnott. Si l'on fait intervenir les caractères (p-adiques) de G, le problème est beaucoup plus compliqué. Il suffit pour s'en convaincre de se rappeler que le passage de la formule analytique donnant la partie "moins" du nombre de classes d'un corps abélien imaginaire, aux formules "caractère (p-adique) par caractère", ne constitue rien d'autre que la Conjecture d'Iwasawa-Leopoldt, dont toute démonstration passe par la Conjecture Principale sous la forme du théorème 3.22 ! (D'ailleurs, notre démonstration utilise aussi la Conjecture Principale).

Un commentaire s'impose à ce stade : ce programme avait déjà été réalisé par Kuz'min dans un long et difficile article [Kuz96] paru peu de temps auparavant avec une démarche par co-descente nettement plus compliquée que la nôtre.

Pour notre part, nous découpons d'abord en ψ-parties au niveau de F (ψ parcourt les caractères de $\mathrm{Gal}(F/\mathbb{Q})$ d'ordre premier à p). Pour cela, nous suivons un raffinement de la méthode de Gillard ([Gil79]). Le bonus est de pouvoir "expliquer" les divers facteurs parasites qui apparaissent, comme étant des "constantes structurelles" attachées aux divers modules. Des applications sont ensuite données à la théorie d'Iwasawa des unités circulaires et des unités semi-locales (essentiellement, des résultats asymptotiques de

structure galoisienne). Enfin, nous proposons, dans l'esprit de [Kuz96], une modification des (p)-unités circulaires qui permet de donner des formules de co-descente sans facteur parasite.

5.1.1 Méthode de Gillard et unités circulaires.

Gillard dans [Gil79] calcule les indices de divers groupes d'unités cyclotomiques, essentiellement construits à partir des "unités formelles" de Leopoldt. Ces modules ont une structure galoisienne plus simple que la version de Sinnott. On obtient des formules d'indice complètement explicites, mais le "facteur parasite" est nettement moins bon que celui de Sinnott (à l'étage n il est divisible par $p^{n\#\Delta}$). Soit F un corps abélien totalement réel. On pose $G = \mathrm{Gal}(F/\mathbb{Q})$. Alors G s'écrit $G = \Delta \times P$ avec $p \nmid \#P$. Dans le sous-paragraphe qui suit, on applique la méthode de Gillard à C_F, avec deux variations :

1. On tient compte de l'indice de structure $(\mathcal{S}(\overline{C}_F) : \overline{C}_F)$ (voir [BN01] définition 1.1 pour la définition du module semi-simplifié associé à un module M et noté $\mathcal{S}(M)$).
2. On doit faire avec la diversité des générateurs de C_F, qui fait intervenir les b_χ de la définition 5.1.

On fixe ψ un caractère $\mathbb{Q}_p$-irréductible de Δ. On note e_ψ l'idempotent de $\mathbb{Z}_p[\Delta] \subset \mathbb{Z}_p[G]$ associé à ψ et pour tout $\mathbb{Z}_p[\Delta]$-module M, on note $M_\psi = e_\psi M$. On note $N_\psi = (\mathcal{S}(\mathbb{Z}_p[G]_\psi) : \mathbb{Z}_p[G]_\psi)$ le (ψ)-indice de structure maximal. Pour tout caractère de Dirichlet χ on note f_χ son conducteur.

Définition 5.1 ([BN01] définition 1.6) *Pour tout nombre premier l divisant* $\mathrm{cond}(F)$*, on fixe un générateur g_l de* $\mathrm{Gal}(F \cap \mathbb{Q}(l^\infty)/\mathbb{Q})$*. Si m est un entier divisant* $\mathrm{cond}(F)$*, et divisible par f_χ on note :*

$$b_{(\chi,m)} = [F : F \cap \mathbb{Q}(\zeta_m)] \prod_{l|m} (1 - \chi(l)^{-1}) \in \overline{\mathbb{Q}_p},$$

où le produit est pris sur les nombres premiers l qui divisent m. On note :

$$b_{(\chi,m,0)} = \begin{cases} b_{(\chi,m)} \text{ si } m \text{ est composé} \\ (1 - \chi(g_l)) b_{(\chi,m)} \quad \text{si } m \text{ est puissance d'un nombre premier } l \end{cases}$$

Soit m_χ (resp. $m_{(\chi,0)}$) l'entier naturel tel que la valuation p-adique de $b_{(\chi,m_\chi)}$ (resp. de $b_{(\chi,m_\chi,0)}$) soit minimale. On note $b_\chi := b_{(\chi,m_\chi)}$ (resp. $b_{(\chi,0)} := b_{(\chi,m_{(\chi,0)},0)}$).

Ces constantes explicites interviennent dans le lemme-clé ci-dessous qui est l'étape essentielle pour la démonstration du théorème 5.4. Dans toutes la suite de ce paragraphe pour a, $b \in \mathbb{Z}_p$ la notation $a \sim b$ signifie que a et b on même valuation p-adique.

Lemme 5.2 ([BN01] Lemme 1.8) *Pour tout caractère χ sur G absolument irréductible on note e_χ l'idempotent associé à χ. Soit $\widetilde{\psi}$ l'ensemble des caractères absolument irréductibles de G divisant ψ (concrètement vérifiant $e_\chi e_\psi \neq 0$). Lorsque ψ est non trivial, on a :*

$$(\mathcal{U}_{F,\psi} : \overline{C}_{F,\psi}) \sim \frac{(\mathcal{S}(\overline{C}_{F,\psi}) : \overline{C}_{F,\psi})}{N_\psi} \prod_{\chi \in \widetilde{\psi}} b_\chi L_p(1,\chi)$$

Lorsque ψ est trivial, on a :

$$(\mathcal{U}_{F,\psi} : \overline{C}_{F,\psi} \oplus (1+p)^{\mathbb{Z}_p}) \sim \frac{[F:\mathbb{Q}](\mathcal{S}(\overline{C}_{F,\psi}) : \overline{C}_{F,\psi})}{N_\psi} \prod_{\chi \in \widetilde{\psi},\ \chi \neq 1} b_{(\chi,0)} L_p(1,\chi)$$

Ce lemme se démontre en utilisant la formule d'analyse p-adique du théorème 3.9 et le principe de calcul d'indices χ-partie par χ-partie avec les indices de structure exposé dans le §1.1 de [BN01]. En comparant la structure galoisienne du réseau $Iw(F)$ et de $\overline{C}_F$ (essentiellement ils sont isomorphes) on obtient une expression du ψ-indice des unités circulaires dans les unités semi-locales. Notons $c_{F,\psi}$ la ψ-partie de la constante de Sinnott définie ci-dessous :

$$c_{F,\psi} = \begin{cases} (\mathbb{Z}_p[G]_\psi : \overline{Iw(K)}_\psi) \text{ si } \psi \neq 1 \\ (\mathbb{Z}_p[G]_\psi : \overline{Iw(K)}_\psi)\ \dfrac{\prod_l [F \cap \mathbb{Q}(l^\infty) : \mathbb{Q}]}{[F:\mathbb{Q}]} \text{ si } \psi = 1 \end{cases}$$

Théorème 5.3 ([BN01] Théorème 2.5)

1. *Si $\psi \neq 1$ on a :*

$$(\mathcal{U}_{F,\psi} : \overline{C}_{F,\psi}) \sim c_{F,\psi} \prod_{\chi \in \widetilde{\psi}} L_p(1,\chi)\ .$$

2. *Si $\psi = 1$ on a :*

$$(\mathcal{U}_{F,\psi} : \overline{C}_{F,\psi} \oplus (1+p)^{\mathbb{Z}_p}) \sim [F:\mathbb{Q}] c_{F,\psi} \prod_{\chi \in \widetilde{\psi}, \chi \neq 1} L_p(1,\chi).$$

Jusqu'ici on n'a utilisé ni la théorie du corps de classes ni la Conjecture Principale. La suite exacte de ramification (R) du §3.3.2 et la Conjecture Principale (sous la forme du théorème 3.19), permettent de passer de l'indice dans les unités semi-locales à l'indice dans les unités globales et de remplacer le produit des $L_p(1,\chi)$ par la ψ-partie de l'ordre du groupe des classes. Il suit :

Théorème 5.4 ([BN01] théorème 2.8) *Soit h_ψ la ψ-partie de la p-partie du nombre de classes de F, on a :*

$$(\overline{U}_{F,\psi} : \overline{C}_{F,\psi}) \sim c_{F,\psi} h_\psi \ .$$

Ce théorème contient en particulier la conjecture de Gras (pour $p \neq 2$) du §2.5 (il suffit de prendre le cas particulier $\Delta = G$).

5.1.2 Idéaux de Fitting et structure galoisienne.

La formule d'indice du théorème 5.4 montre que la ψ-partie du groupe des classes d'idéaux $X_{F,\psi}$ et celles du groupe des classes d'unités $(\overline{U}_F/\overline{C}_F)_\psi$ ont essentiellement le même ordre. On a vu que cette démonstration ne repose pas sur un isomorphisme, ne serait ce qu'à cause des cas de non-trivialité de la constante $c_{F,\psi}$. En montant dans la $\mathbb{Z}_p$-tour F_∞/F et en étudiant l'action de G_n on va établir des relations plus algébriques d'abord entre les groupes $\mathcal{U}_n/\overline{C}_n$ et $\mathfrak{X}_n$; puis entre X_n et $\overline{U}_n/\overline{C}_n$. On procède par co-descente en comparant $(\mathcal{U}_\infty/\overline{C}_\infty)_{\Gamma_n}$ avec $\mathcal{U}_n/\overline{C}_n$. Évidemment les morphismes naturels entre ces deux modules ne sont en général pas des isomorphismes. Posons $\ker(\psi) = \{\delta \in \Delta | \psi(\delta) = \psi(1)\}$. Si p n'est pas totalement décomposé dans le sous corps $F^{P\ker(\psi)}$ de F fixé par $\ker(\psi)$ et P, alors le morphisme $(\mathcal{U}_\infty/\overline{C}_\infty)_{\Gamma_n,\psi} \longrightarrow (\mathcal{U}_n/\overline{C}_n)_\psi$ est surjectif. On va utiliser cette hypothèse : abrégeons-la par $\psi(p) \neq 1$. Soit A_ψ l'anneau $e_\psi \mathbb{Z}_p[\Delta]$. Alors $(\mathcal{U}_n/\overline{C}_n)_\psi$ et $(\mathfrak{X}_n)_\psi$ sont des $A_\psi[G_n]$-modules.

Théorème 5.5 ([BN01] Théorème 3.3) *On suppose que le couple (F,p) satisfait (gHB) et soit ψ un caractère $\mathbb{Q}_p$-irréductible de Δ tel que $\psi(p) \neq 1$. Alors, pour tout $n \geq 0$, on a :*

1. *$c_{F_n,\psi} = 1$.*
2. *Les modules $(\mathcal{U}_n/\overline{C}_n)_\psi$ et $(\mathfrak{X}_n)_\psi$ ont même idéal de Fitting sur l'algèbre $A_\psi[G_n]$.*

Ce théorème généralise un résultat de Cornacchia ([Cor98] theorem 2). La version publiée dans [BN01] ne mentionne pas l'hypothèse (gHB). C'est une erreur qui depuis a été corrigée p. 86 de [BN05]. La propriété 1. indique que

la constante de Sinnott se "concentre" en les caractères ψ qui décomposent totalement p. Donc, pour les autres caractères, les ordres de $(\overline{U}_n/\overline{C}_n)_\psi$ et de $X_{n,\psi}$ sont égaux. En étudiant et en comparant les propriétés fines de ces objets, j'ai l'impression qu'ils se comportent un peu comme des groupes en dualité. Évidemment l'existence d'une telle dualité suppose la trivialité des constantes de Sinnott. On sait que les groupes finis en dualité sont isomorphes (non canoniquement). Sous la conjecture de Greenberg les modules X_∞ et $\overline{U}_\infty/\overline{C}_\infty$ sont finis. On pourrait donc espérer que la conjecture de Greenberg entraîne l'existence d'un isomorphisme entre X_∞ et $\overline{U}_\infty/\overline{C}_\infty$. Dans cet ordre d'idée on a le théorème

Théorème 5.6 ([BN01] Théorème 3.5) *On suppose que le couple (F,p) satisfait (gHB) et soit ψ un caractère $\mathbb{Q}_p$-irréductible de Δ tel que $\psi(p)\neq 1$. On suppose la conjecture de Greenberg pour F et p. Alors il existe un rang $N\in\mathbb{N}$ tel que pour tout $n\geq N$, $(X_n)_\psi$ et $(\overline{U}_n/\overline{C}_n)_\psi$ sont isomorphes (comme modules galoisiens).*

Ce théorème généralise des résultats de [KS95] et [Oza97]. Les résultats de cette sous-section s'appliquent uniquement aux caractères ψ ne décomposant pas p. Que dire des caractères décomposant p ? Dans le §4 de [BN01] on propose une modification $\overline{C}''_\infty$ des unités circulaires au niveau infini, et par co-descente de cette modification un sous-module $\widetilde{C}''_n$ de $\overline{U}'_n$. On arrive avec cette modification, pour tout caractère non-trivial, à des énoncés analogues à ceux des théorèmes 5.6 et 5.5 (mais l'hypothèse (gHB) omise dans cette partie doit être rajoutée). Ces résultats ne sont pas satisfaisants. D'abord parce que les modifications proposées ne sont pas du tout explicites, ensuite parce que rien n'est dit au sujet d'un caractère ψ trivial. Il est connu (phénomènes des zéros triviaux) qu'aux caractères décomposant p, la co-descente en théorie d'Iwasawa est bien plus compliquée. L'astuce pour contourner les zéros triviaux est due originellement à Solomon et consiste à remplacer le co-descendu des unités circulaires (ici trivial !) par celui des p-unités circulaires modifiées. Je reviens sur cette construction dans la section suivante (qui concerne F pour p totalement décomposé dans F).

5.2 Unités circulaires modifiées.

Dans cette section on suppose F totalement réel et p totalement décomposé dans F. En particulier $\psi(p)=1$ pour tout ψ et les théorèmes 5.6 et 5.5 ne donnent aucune information sur l'arithmétique de F. Notre principal but dans l'article [BN05] est de présenter une construction alternative des p-unités circulaires modifiées définies dans [Sol92]. L'essentiel de notre apport

est de "fonctorialiser" la construction élément par élément de Solomon. En d'autres termes nous travaillons avec des homomorphismes et des modules. Cela permet de comparer les modules d'Iwasawa avec leurs analogues au niveau fini par des homomorphismes naturels mais non triviaux (au contraire de ceux obtenus par co-descente naïve). De plus, ces homomorphismes, en conjonction avec la machinerie des "unités spéciales" à la Rubin (on dirait plutôt aujourd'hui "systèmes d'Euler") nous permettent de démontrer un résultat d'annulation de classes réelles conjecturé par Solomon.

5.2.1 Hilbert 90 en Théorie d'Iwasawa.

Pour tout v divisant p, on note $\widehat{F}_v^\times$ le sous-groupe de $\overline{F_v^\times}$ qui correspond par la théorie du corps de classe à la $\mathbb{Z}_p$-extension cyclotomique $F_{v,\infty}/F_v$; c'est-à-dire $\overline{F_v^\times}/\widehat{F}_v^\times \simeq \mathrm{Gal}(F_{v,\infty}/F_v)$. Le groupe $\widehat{F}_v^\times$ est parfois appelé groupe des normes universelles (cyclotomiques) de $F_{v,\infty}/F_v$. Soit

$$\delta : \overline{U}'_F \longrightarrow \oplus_{v\in S}\overline{F_v^\times}/\widehat{F}_v^\times,$$

l'homomorphisme provenant du morphisme diagonal.

Définition 5.7 *On appelle* Noyau de Gross *([FGS81]; voir aussi [Kuz72]) et on note $\widehat{U}'_F$ le noyau de δ :*

$$\widehat{U}'_F = \ker \delta.$$

Les éléments de $\widehat{U}'_F$ sont les (p)-unités de F qui localement sont normes universelles cyclotomiques en toute place.

Dans la terminologie logarithmique de Jaulent le nombre p fixé dans ce mémoire est noté ℓ. Le groupe $\widehat{U}'_F$ est noté $\widetilde{\mathcal{E}}_F$ et appelé "ℓ-groupe des unités logarithmiques" (voir par exemple [Jau94] définition 3.1 et proposition 3.2) ; le groupe $(X'_\infty)_\Gamma$ est noté $\widetilde{Cl}_F$ et appelé "ℓ-groupe des classes logarithmiques". L'approche logarithmique permet d'expliciter δ et donc d'étudier son co-noyau. La finitude de ce co-noyau est équivalente à la conjecture de Gross généralisée ([Jau94] théorème & conjecture 2.3). Dans le contexte abélien totalement réel de ce mémoire la conjecture de Gross généralisée est une conséquence de la conjecture de Leopoldt et on s'intéresse d'abord au noyau de δ. Le point de départ de notre construction des (p)-unités circulaires modifiées est un lemme très simple :

Lemme 5.8 ([BN05] lema 1.1)

$$\widehat{U}'_F \cap \overline{U}_F = \{1\}$$

Ce lemme permet d'abord de cerner le problème : les unités de F provenant de la descente "naïve" sont toutes dans $\widehat{U}'_F$ donc triviales. Autrement dit le morphisme naturel $\overline{U}_\infty \longrightarrow \overline{U}_F$ est trivial. Mais un théorème de Kuz′min affirme l'injectivité du morphisme naturel $(\overline{U}'_\infty)_\Gamma \hookrightarrow \overline{U}'_F$. En particulier le noyau du morphisme naturel $\overline{U}'_\infty \longrightarrow \overline{U}'_F$ est égal à $(\gamma-1)\overline{U}'_\infty$ pour tout γ (à partir de maintenant fixé) engendrant Γ. Cela permet de démontrer le théorème (de division par T) :

Théorème 5.9 ([BN05] theorem 2.7 et corollary 2.8) *Soit* $(\overline{U}'_\infty)^{(0)} = \ker(\overline{U}'_\infty \longrightarrow \overline{U}'_F)$ *le noyau du morphisme de descente naïve. La multiplication par* $(\gamma-1)$ *donne un isomorphisme de* Λ*-modules :*

$$\overline{U}'_\infty \xrightarrow{\sim} (\overline{U}'_\infty)^{(0)} = \overline{U}_\infty.$$

Le morphisme réciproque à celui de ce théorème revient essentiellement à diviser par $T = \gamma - 1$, ce qui ne serait pas possible sans ce théorème. On peut maintenant définir des morphismes de descente non triviaux :

Définition 5.10 ([BN05] definition 2.9)

1. *On définit :*

$$\Theta\colon \overline{U}_\infty \xrightarrow{\sim} \overline{U}'_\infty \xrightarrow{nat.} \left(\overline{U}'_\infty\right)_\Gamma \hookrightarrow \overline{U}'_F.$$

   Le premier isomorphisme est l'inverse de celui du théorème 5.9 ; la dernière injection vient du théorème de Kuz′min. La définition de Θ *dépend du choix de* γ*.*

2. *On définit* $\Theta_C\colon \overline{C}_\infty \longrightarrow \overline{U}'_F$ *comme la restriction de* Θ *à* $\overline{C}_\infty$*.*

Le morphisme Θ_C redonne les (p)-unités de Solomon ([Sol92]) à moindre coût. En fait le choix de tout élément intéressant de $\overline{C}_\infty$ fournit par Θ_C un élément intéressant de $\overline{U}'_F$. Précisément si on reprend la suite d'unités circulaires $\varepsilon_\infty(\mathcal{P})$ du §4.4, alors on obtient en conséquence des définitions $\Theta_C(\varepsilon_\infty(\mathcal{P})) = \kappa(F,c)$, où $\kappa(F,c)$ est l'unité construite dans [Sol92]. En exploitant le morphisme Θ_C on re-démontre et généralise diverses formules de rang et d'indice contenus dans [Sol92]. Mais cette construction a aussi beaucoup d'autres applications. Parmi ces applications j'en détaille deux dans les sous-sections à venir.

5.2.2 Annulations de classes d'idéaux réelles.

Un problème intéressant, accessible et encore ouvert est de décrire le Fitting initial, voire l'annulateur dans $\mathbb{Z}_p[G]$ des modules X_F et $\overline{U}_F/\overline{C}_F$

(ces idéaux doivent être liés). Je vais maintenant énoncer une conjecture de Solomon dans cet ordre d'idées. Pour cela je renonce temporairement à l'hypothèse p totalement décomposé et je suppose seulement que F est abélien et que p est non ramifié dans F. Notons $\imath\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$, le plongement fixé depuis le §3.2 et soit $\mathcal{O}$ l'adhérence dans $\mathbb{C}_p$ in $\mathbb{Q}_p^{\text{sep}}$). Pour chaque sous-corps $M \neq \mathbb{Q}$ de F, on définit un *élément de Solomon* sol_M comme dans [Sol92], §4 :

$$\text{sol}_M := \frac{1}{p} \sum_{g \in \text{Gal}(M/\mathbb{Q})} \left(\log_p(\imath(\varepsilon_M^g))\right) g^{-1} \in \mathcal{O}[\text{Gal}(M/\mathbb{Q})].$$

Par convention $\text{sol}_{\mathbb{Q}} = 1$. Ces éléments doivent être considérés comme les analogues totalement réels des éléments de Stickelberger ξ_n du §3.2.2. En effet le théorème de Solomon ([Sol92], theorem 2.1) montre que ces éléments sont construit sur les valuations p-adiques des "sommes de Gauß" totalement réelles $\kappa(F, c) = \Theta_C(\varepsilon_\infty(\mathcal{P}))$. Et l'analogue totalement réel du théorème de Stickelberger est la conjecture de Solomon :

Conjecture 5.11 (voir [Sol92], conjecture 4.1) sol_F *annule* $Cl_F \otimes \mathcal{O}$.

Cette conjecture est vraie dans le cas "semi-simple" (i.e. $p \nmid [F : \mathbb{Q}]$), mais n'apporte rien de nouveau puisque dans ce cas c'est une conséquence directe de la Conjecture Principale (théorème 3.19) comme expliqué dans les commentaires suivant 4.1 de [Sol92]. Pour le cas général introduisons un élément de Solomon modifié :

Définition 5.12 ([BN05] definition 5.2) *Soit F un corps abélien totalement réel dans lequel p est non ramifié. Soit $w \mid p$ la place de F correspondant au plongement $\imath$. Par abus de notation on note encore w pour la place correspondante de tout sous-corps M de F.*

1. *Soit $M \subset F$. Soit $\widetilde{\text{sol}}_M^F$ un quelconque élément de $O_{F_w}[\text{Gal}(F/\mathbb{Q})]$ qui redonne $\text{sol}_M \in O_{M_w}[\text{Gal}(M/\mathbb{Q})] \subset O_{F_w}[\text{Gal}(M/\mathbb{Q})]$ par restriction. On définit sol_M^F par la formule (la multiplication est celle de l'anneau commutatif $O_{F_w}[\text{Gal}(F/\mathbb{Q})]$) :*

$$\text{sol}_M^F := \widetilde{\text{sol}}_M^F \times \text{Tr}_{F/M}.$$

   Ce produit ne dépend plus du choix du relevé $\widetilde{\text{sol}}_M^F$.

2. *Pour tout corps abélien réel M tel que $\text{cond}(M)$ est puissance d'un seul nombre premier, on fixe un générateur g_M du groupe cyclique*

$\mathrm{Gal}(M/\mathbb{Q})$. *Pour tout sous-corps* M *de* F *on définit :*

$$\mathrm{sol}^F_{M,2} := \begin{cases} (1-g_M)\,\mathrm{sol}^F_M & \textit{si } \mathrm{cond}(M) \textit{ est puissance d'un seul} \\ \textit{nombre premier,} & \\ \mathrm{sol}^F_M & \textit{sinon.} \end{cases}$$

Avec cet élément de Solomon modifié (i.e. augmenté par $1-g_F$ lorsque le conducteur de F est puissance d'un seul nombre premier) on démontre dans [BN05], pour le cas particulier crucial p totalement décomposé dans F, le théorème :

Théorème 5.13 ([BN05] theorem 5.4) *Pour tout corps abélien* F *totalement réel et tout* p *totalement décomposé dans* F *:*

$$\mathrm{sol}^F_{F,2}\, X_F = \{0\}.$$

Ce théorème se démontre directement en utilisant la technique maintenant classique des systèmes d'Euler [Rub87] et cette démonstration peut se faire directement avec la définition de $\kappa(F,c)$ et sans la construction naturelle du §5.2.1. Si le conducteur de F est divisible par deux nombres premiers distincts ceci est la conjecture de Solomon, parce que par définition même dans ce cas $Cl_F \otimes \mathcal{O} = X_F$ et $\mathrm{sol}^F_{F,2} = \mathrm{sol}_F$. Lorsque le conducteur de F est puissance d'un seul nombre premier ℓ ce théorème est légèrement plus faible que la conjecture 5.11. Par contre c'est l'analogue exact d'un théorème d'annulation pour les classes d'unités que j'énonce dans la sous-section suivante.

5.2.3 Idéaux de Fitting de classes d'unités.

Dans cette sous-section on suppose à nouveau p totalement décomposé dans F. Les éléments définis explicitement dans la définition 5.12 permettent de définir des idéaux de $\mathbb{Z}_p[G]$.

Définition 5.14 ([BN05] definition 5.5) *On définit les idéaux* $\mathrm{Sol}_2(F) \subset \mathrm{Sol}_1(F)$ *dans* $\mathbb{Z}_p[G]$ *par les systèmes de générateurs suivants :*

$$\mathrm{Sol}_1(F) := \left\langle \mathrm{sol}^F_M \,|\mathbb{Q} \subseteq M \subseteq F \right\rangle$$

$$\mathrm{Sol}_2(F) := \left\langle \mathrm{sol}^F_{M,2} \,|\mathbb{Q} \subseteq M \subseteq F \right\rangle.$$

Ces idéaux sont les idéaux de Fitting de deux quotients de $(\mathcal{U}_\infty)_\Gamma$.

Théorème 5.15 ([BN05] theorem 5.7) *On suppose* F *abélien totalement réel et* p *totalement décomposé dans* F*.*

1. *On a un isomorphisme*

$$(\mathcal{U}_\infty/\overline{C}_\infty)_\Gamma \cong \frac{\mathbb{Z}_p[G]}{\mathrm{Sol}_1(F)}.$$

En particulier $\mathrm{Sol}_1(F)$ *est le Fitting initial de* $(\mathcal{U}_\infty/\overline{C}_\infty)_\Gamma$.

2. $\mathrm{Sol}_2(F)$ *annule* $\overline{U}_F/\overline{C}_F$.

Dans le théorème 5.7 on réalise aussi $\mathrm{Sol}_2(F)$ comme le Fitting initial d'un quotient de $(\mathcal{U}_\infty)_\Gamma$. Ce quotient contient comme sous-module $\overline{U}_F/\overline{C}_F$, ce qui montre le 2. J'ai préféré, dans ce mémoire, simplifier les énoncés (quitte à affaiblir les résultats).
Question : $\mathrm{Sol}_1(F)$ annule-t-il $\overline{U}_F/\overline{C}_F$?

Corollaire 5.16 ([BN05] corollary 5.8) *On note* $\kappa_F := \#\mathrm{Tor}_{\mathbb{Z}_p}((\overline{C}_\infty)_\Gamma)$ *et* R_F^{Leop} *le régulateur de Leopoldt de* F.

$$(\mathbb{Z}_p[G] : \mathrm{Sol}_1(F)) = \kappa_F \#\mathrm{Tor}_{\mathbb{Z}_p}\mathfrak{X}_F \sim \kappa_F h_F R_F^{Leop} p^{1-[F:\mathbb{Q}]}$$

Cette formule donne un analogue totalement réel de la formule d'indice de l'idéal de Stickelberger (voir la première partie de l'article [Sin80] par exemple). Ici la constante κ_F, qui est triviale sous l'hypothèse (gHB), joue le rôle de la constante de Sinnott.

5.2.4 Un critère pour la conjecture de Greenberg.

La conjecture de Greenberg dont il a été question en §3.3.4 a été vérifiée par des calculs numériques pour énormément de corps abéliens. Parmi ces corps les cas de décomposition de p étaient soigneusement évités et considérés comme très difficiles (jusqu'aux résultats de Taya [Ta99]). Cette difficulté supplémentaire est probablement liée au phénomène des "zéros triviaux" que nous venons de contourner. Toujours est-il que l'approche explicite et canonique développée au paragraphe 5.2.1 permet de retrouver plus simplement le critère de Taya pour la conjecture de Greenberg dans le cas p totalement décomposé (voir [Ta99], theorem 1.3 ; Taya utilise seulement la conjecture de Leopoldt) :

Théorème 5.17 *Soit* F *un corps abélien totalement réel et soit* p *un nombre premier impair totalement décomposé dans* F. *On note* $D_n \subset X_n$ *le sous-module engendré par les images des places de* F_n *divisant* p. *Alors la conjecture de Greenberg pour* F *et* p *est vraie si et seulement si*

$$\#D_n = \#\mathrm{tor}_{\mathbb{Z}_p}(\mathfrak{X}_F)$$

pour tout n *assez grand.*

5.3 Co-descente pour les classes d'unités.

Les suites de groupe de classes d'idéaux X_n et $\mathfrak{X}_n$ sont depuis le début, et à bon escient, au cœur de la théorie d'Iwasawa. La co-descente pour $\mathfrak{X}_n$ est tautologique ce qui, en soi, avec la proximité entre $\mathfrak{X}_n$ et X_n, justifie l'intérêt porté à ce module. Le fait que X_n co-descende (asymptotiquement) bien suit du théorème d'Iwasawa (théorème 3.6). Par contre les suites des groupes de classes d'unités $\overline{U}_n/\overline{C}_n$ et $\mathcal{U}_n/\overline{C}_n$ ont (à mon avis à tort) moins souvent été étudiées pour elles-même. Dans l'article [Bel05] je borne uniformément avec n et *sans utiliser la Conjecture Principale*, l'ordre des noyaux et co-noyaux des applications naturelles

$$(\mathcal{U}_\infty/\overline{C}_\infty)_{\Gamma_n} \longrightarrow \mathcal{U}_n/\overline{C}_n$$

et

$$(\overline{U}_\infty/\overline{C}_\infty)_{\Gamma_n} \longrightarrow \overline{U}_n/\overline{C}_n.$$

J'en déduis l'analogue pour les classes d'unités du théorème d'Iwasawa pour les classes d'idéaux. Le même résultat est démontré dans l'article [Ngu05] en utilisant la Conjecture Principale. Ultérieurement, et toujours en utilisant la Conjecture Principale, Lescop Movahhedi et Nguyen Quang Do ont dévissé ces noyaux et co-noyaux dans le corps de [LMN].

5.3.1 Conséquence de la conjecture de Leopoldt.

Comme dans tout ce mémoire, F désigne un corps abélien réel, $p \neq 2$ le nombre premier fixé et $G = \mathrm{Gal}(F/\mathbb{Q})$. Soit $M_\infty = \varprojlim(M_n)$ un Λ-module (Par exemple $M_n = \overline{U}_n, \overline{C}_n, \mathcal{U}_n \dots$). Bien sur les projections $M_\infty \longrightarrow M_n$ se factorisent à travers $(M_\infty)_{\Gamma_n} \longrightarrow M_n$, mais en général ces morphismes ont des noyaux et co-noyaux non triviaux. On va noter $\mathrm{Ker}_n(M_\infty)$ pour le noyau $\mathrm{Ker}_n(M_\infty) = \ker((M_\infty)_{\Gamma_n} \longrightarrow M_n)$, $\widetilde{M_n} \subset M_n$ pour l'image $\widetilde{M_n} = \mathrm{Im}((M_\infty)_{\Gamma_n} \longrightarrow M_n)$ et $\mathrm{Coker}_n(M_\infty) = M_n/\widetilde{M_n}$ pour le co-noyau. Bien sûr ces trois objets dépendent de la suite (M_n) et pas seulement de sa limite M_∞ mais j'étudie uniquement des suites provenant de l'arithmétique des F_n et ces notations n'introduisent aucune ambiguïté. Avant d'étudier des propriétés plus précises des noyaux Ker_n et co-noyaux Coker_n de co-descentes des classes d'unités j'établis leur finitude en utilisant la conjecture de Leopoldt et le théorème de Tsuji (voir la proposition-définition 3.16 et le théorème 3.17) qui sont en amont de la Conjecture Principale.

Théorème 5.18 ([Bel05] theorem 1.1) *On fixe un générateur γ du groupe de Galois $\Gamma = \mathrm{Gal}(F_\infty/F)$. On rappelle que la notation $g_{\theta,\gamma}(T)$ désigne*

la série d'Iwasawa-Coleman-Tsuji associée au caractère de première espèce θ (voir la proposition-définition 3.16).

1. *On suppose que p est au plus modérément ramifié dans F. Alors à une puissance de p près l'idéal caractéristique de $\mathcal{U}_\infty/\overline{C}_\infty$ est engendré par le produit :* $\prod_{\theta\in\widehat{G},\theta\neq 1} g_{\theta,\gamma}(T)$.
2. *En toute généralité et pour tout $n\in\mathbb{N}$, les Γ_n-co-invariants $(\mathcal{U}_\infty/\overline{C}_\infty)_{\Gamma_n}$ et $(\overline{U}_\infty/\overline{C}_\infty)_{\Gamma_n}$ sont finis.*

Ce théorème fait partie du folklore depuis bien longtemps (Iwasawa et Coleman avaient traité le cas $F=\mathbb{Q}(p)^+$). Je ne connais pas de référence contenant une démonstration complète et générale de ces affirmations et j'ai donné une démonstration p.3 et 4 de [Bel05]. La version de [Bel05], malheureusement déjà soumise, comporte deux erreurs mineures qui sont corrigées dans les versions jointes et seront corrigées dans l'article définitif avant sa publication. Je précise ces erreurs et leurs corrections :

- L'hypothèse "$\mathbb{B}_\infty\cap F=\mathbb{Q}$" dans 1. doit être remplacée par "p modérément ramifié dans F", de sorte que tous les caractères de $\widehat{G}$ soient de première espèce (c'est la seconde hypothèse, plus restrictive, qui est utilisée dans [Tsu99]). Cela ne change rien à la démonstration de 1. et 2.
- Ligne -14 p.3 l'affirmation "T divides no generator of the two characteristic ideals" doit être remplacée par "both characteristic ideals are prime to all $(T+1)^{p^n}-1$ for all $n\in\mathbb{N}$". La conjecture de Leopoldt dans la formulation "$L_p(1,\chi)\neq 1$" donne aussi cette seconde condition pour la série $g_{\theta,\gamma}(T)$. En effet pour θ fixé soit ζ une racine de l'unité d'ordre une puissance de p, reprenons le choix de γ du corollaire 3.18 et soit ψ l'unique caractère de seconde espèce tel que $\psi(\gamma)=\zeta^{-1}$. Alors on a $g_{\theta,\gamma}(\zeta-1)=f(\zeta^{-1}(1+dp)-1,\theta)=L_p(1,\theta\psi)\neq 0$, et donc $g_{\theta,\gamma}$ est premier avec le polynôme minimal de $\zeta-1$. Le reste de la démonstration de 5.18 donnée dans [Bel05] ne change pas.

Après avoir démontré que $(\mathcal{U}_\infty/\overline{C}_\infty)_{\Gamma_n}$ et $(\overline{U}_\infty/\overline{C}_\infty)_{\Gamma_n}$ sont finis (et donc aussi les deux Ker_n concernés) je passe en revue les propriétés de descente des modules multiplicatifs locaux et semi-locaux habituels dans le §2 de [Bel05]. Ensuite je reviens aux classes d'unités.

5.3.2 Noyaux et co-noyaux de descente.

Je démontre que la descente fonctionne bien (asymptotiquement) pour les modules $M_\infty=\overline{U}_\infty/\overline{C}_\infty$ ou (ce qui est équivalent pour $M_\infty=\mathcal{U}_\infty^{(0)}/\overline{C}_\infty$

(voir les explications et la notation ci-dessous pour le symbole $^{(0)}$). Cela signifie que pour chacun de ces deux cas $\mathrm{Ker}_n(M_\infty)$ et $\mathrm{Coker}_n(M_\infty)$ sont finis et d'ordre bornés avec n. Ma stratégie est la suivante. D'abord je démontre que borner les noyaux (resp. les co-noyaux) d'un module est équivalent à borner les noyaux (resp. les co-noyaux) de l'autre. Puis j'utilise la trivialité des $\mathrm{Ker}_n(\overline{U}'_\infty)$ (théorème de Kuz′min [Kuz72], theorem 7.3) pour borner les $\mathrm{Ker}_n(\overline{U}_\infty/\overline{C}_\infty)$. Enfin j'utilise la théorie du corps de classes local pour borner les co-noyaux de descente pour $\mathcal{U}_\infty^{(0)}/\overline{C}_\infty$. Avant tout cela je modifie légèrement la suite $\mathcal{U}_n/\overline{C}_n$. En effet, pour tout n, le module $\mathcal{U}_n/\overline{C}_n$ est (par la conjecture de Leopoldt) de $\mathbb{Z}_p$-rang 1 alors que $(\mathcal{U}_\infty/\overline{C}_\infty)_{\Gamma_n}$ est de torsion. Ce rang 1 vient $N_{K_n/\mathbb{Q}}(\overline{U}_n) = \{0\}$, ou encore du point de vue de la théorie du corps de classes il correspond au rang de la $\mathbb{Z}_p$-extension F_∞/F. On pose la

Notation : Soit K un corps de nombres. Dans tout ce qui suit $\mathcal{U}_F^{(0)}$ désignera le noyau de

$$N_{K/\mathbb{Q}} \colon \mathcal{U}_K \longrightarrow \mathcal{U}_\mathbb{Q}.$$

De façon cohérente on notera $\mathcal{U}_n^{(0)}$ pour le noyau de $N_{F_n/\mathbb{Q}}$ et $\mathcal{U}_\infty^{(0)} = \varprojlim \mathcal{U}_n^{(0)}$.

Par la théorie du corps de classes local on a $\widetilde{\mathcal{U}}_n \subset \mathcal{U}_n^{(0)}$ et en particulier $\mathcal{U}_\infty = \varprojlim(\mathcal{U}_n^{(0)})$. De plus $\mathcal{U}_n^{(0)}/\overline{C}_n$ est de torsion et puisque $N_{F_n/\mathbb{Q}}(\mathcal{U}_n)$ est sans torsion on a $\mathcal{U}_n^{(0)}/\overline{C}_n = \mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{U}_n/\overline{C}_n)$, et de même $\mathcal{U}_n^{(0)}/\overline{U}_n = \mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{U}_n/\overline{U}_n)$. Pour toute ces raisons il est clairement plus agréable de travailler avec la suite $(\mathcal{U}_n^{(0)})_{n\in\mathbb{N}}$ en lieu et place de $(\mathcal{U}_n)_{n\in\mathbb{N}}$, et c'est ce que je fais à partir de maintenant. Cela définit les notations $\widetilde{\mathcal{U}}_n^{(0)}$, $\ker_n(\mathcal{U}_\infty^{(0)})$, $\mathrm{Coker}_n(\mathcal{U}_\infty^{(0)})$ et de même pour les suites $\mathcal{U}_n^{(0)}/\overline{C}_n$, $\mathcal{U}_n^{(0)}/\overline{U}_n$ etc... Bien entendu seuls les différents Coker_n changent vraiment lorsqu'on remplace $\mathcal{U}_n$ par $\mathcal{U}_n^{(0)}$.

Lemme 5.19 ([Bel05] lemma 3.3)

1. $\mathrm{Ker}_n(\overline{U}_\infty/\overline{C}_\infty)$ *et* $\mathrm{Ker}_n(\mathcal{U}_\infty^{(0)}/\overline{C}_\infty)$ *sont finis. Leurs ordres sont bornés (uniformément en n) simultanément ou pas.*
2. $\mathrm{Coker}_n(\overline{U}_\infty/\overline{C}_\infty)$ *et* $\mathrm{Coker}_n(\mathcal{U}_\infty^{(0)}/\overline{C}_\infty)$ *sont finis. Leurs ordres sont bornés (uniformément en n) simultanément ou pas.*

Lemme 5.20 ([Bel05] lemma 4.1)

1. *Les ordres de* $\mathrm{Ker}_n(\overline{U}_\infty/\overline{C}_\infty)$ *sont bornés (uniformément en n).*
2. *Les ordres de* $\mathrm{Ker}_n(\mathcal{U}_\infty^{(0)}/\overline{C}_\infty)$ *sont bornés (uniformément en n).*

Le 1 du lemme 5.20 se reformule en :

Corollaire 5.21 ([Bel05] corollary 4.2) *$\exists c, N \in \mathbb{N}$ tel que pour tout $n \geq N$ on ait les inégalités $|(\overline{U}_\infty/\overline{C}_\infty)_{\Gamma_n}| \leq c|\overline{U}_n/\overline{C}_n|$.*

En comparant avec l'ordre asymptotique de $\overline{U}_n/\overline{C}_n$ donné par la formule d'indice de Sinnott et le théorème d'Iwasawa j'obtiens (avec une preuve plus courte) le théorème de Greither :

Théorème 5.22 ([Bel05] theorem 4.5) *L'invariant structurel μ du module $\overline{U}_\infty/\overline{C}_\infty$ est nul.*

Ce théorème est aussi démontré par Greither dans l'appendice de l'article [FG04]. La démonstration par Greither est différente parce qu'il n'utilise pas la conjecture de Leopoldt et doit donc affronter des $|(\overline{U}_\infty/\overline{C}_\infty)_{\Gamma_n}|$ éventuellement infinis. Pour contourner cette difficulté Greither doit introduire la notion de suite "modérée" (grosso modo cela signifie que ces suites donnent à la limite des modules sans invariant μ).

L'ultime étape dans la codescente est le lemme :

Lemme 5.23 ([Bel05] lemma 5.1)

1. *Les ordres $|\operatorname{Coker}_n(\overline{U}_\infty/\overline{C}_\infty)|$ sont bornés (uniformément avec n).*
2. *Les ordres $|\operatorname{Coker}_n(\mathcal{U}_\infty^{(0)}/\overline{C}_\infty)|$ sont bornés (uniformément avec n).*

5.3.3 Le théorème d'Iwasawa pour les classes d'unités.

En réunissant les lemmes 5.23 et 5.20 on obtient le théorème

Théorème 5.24 ([Bel05] theorem 6.1)

1. *Soient λ_1 et μ_1 les invariants d'Iwasawa des modules $\overline{U}_\infty/\overline{C}_\infty$. Alors $\mu_1 = 0$ et les ordres des $\overline{U}_n/\overline{C}_n$ sont asymptotiquement équivalents à $p^{\lambda_1 n}$.*
2. *Soient λ_2 et μ_2 les invariants d'Iwasawa des modules $\mathcal{U}_\infty/\overline{C}_\infty$. Alors $\mu_2 = 0$ et les ordres des $\mathcal{U}_n^{(0)}/\overline{C}_n$ sont asymptotiquement équivalents à $p^{\lambda_2 n}$.*

Ce théorème est l'exact analogue pour les classes d'unités du théorème d'Iwasawa pour les classes d'idéaux. Par la formule d'indice de Sinnott on sait que ces deux groupes de classes ont des ordres asymptotiquement équivalents et par la Conjecture Principale (dans la formulation du théorème 3.19) on sait aussi que ces modules ont même invariants λ et μ. Le théorème 5.24 est donc une conséquence directe de la Conjecture Principale. Cependant cette objection se retourne. En effet par la formule d'indice de Sinnott les ordres des X_n et de $\overline{U}_n/\overline{C}_n$ sont asymptotiquement équivalents. Donc en utilisant le théorème d'Iwasawa et le théorème 5.24 on obtient *sans utiliser la Conjecture Principale* le corollaire :

Corollaire 5.25 ([Bel05] corollary 6.2)

1. *Les Λ-modules $\overline{U}_\infty/\overline{C}_\infty$ et X_∞ ont mêmes invariants λ et μ.*
2. *Les Λ-modules $\mathcal{U}_\infty^{(0)}/\overline{C}_\infty$ et $\mathfrak{X}_\infty$ ont mêmes invariants λ et μ.*

Dans la démonstration par le système d'Euler cyclotomique de la Conjecture Principale on procède ainsi. On commence par utiliser la machinerie des système d'Euler pour "majorer le groupe des classes" et on démontre que $\mathrm{car}(X_\infty)(\theta)$ divise $\mathrm{car}(\overline{U}_\infty/\overline{C}_\infty)(\theta)$ (pour tout θ de première espèce) comme c'est fait en toute généralité dans [Gre92]. Il faut ensuite se raccrocher aux formules analytiques du nombre de classes pour avoir la divisibilité réciproque. À ce stade de la démonstration le corollaire 5.25 suffit et donne une démonstration directe (entièrement en partie +) de la Conjecture Principale.

Pour comparaison voici le plan de la fin de la démonstration classique telle que ébauchée dans le début de §3 de [Gre92]. Il faut d'abord utiliser la dualité de Kummer pour parvenir aux formulations concernant la partie moins du groupe des classes (voir §3.3.4). Ensuite on utilise le théorème d'Iwasawa pour montrer l'équivalence asymptotique entre les ordres de la suite des co-descendus de X_∞^- et des X_n^-. Enfin les ordres de X_n^- sont donnés en termes du degré de Weierstraß du produit des séries $f(T,\theta)$ grâce à la formule analytique du nombre de classes (partie $-$).

Bibliographie

[Ax65] J. Ax, *On the units of an algebraic number field*, Illinois J. Math. **9** (1965), 584–589.

[Bas66] H. Bass, *Generators and relations for cyclotomic units*, Nagoya Math. J. **27** (1966), 401–407.

[Belt] T. Beliaeva, *unités semi-locales modulo sommes de Gauß en théorie d'Iwasawa*, Thèse de l'université de Franche-Comté Besançon (2004).

[Bel97] J.-R. Belliard, *Sur la structure galoisienne des unités circulaires dans les $\mathbb{Z}_p$-extensions*, Thèse de l'université Bordeaux I (1997).

[Bel98] ———, *Sur la structure galoisienne des unités circulaires dans les $\mathbb{Z}_p$-extensions*, J. Number Theory **69** (1998), no. 1, 16–49.

[Bel02] ———, *Sous-modules d'unités en théorie d'Iwasawa*, Théorie des nombres, Années 1998/2001, Publ. Math. UFR Sci. Tech. Besançon, 2002, 12 p.

[Bel05] ———, *Global units modulo circular units : descent without Iwasawa's Main Conjecture*, preprint (2005).

[BN01] ——— et T. Nguyễn-Quang-Đỗ, *Formules de classes pour les corps abéliens réels*, Ann. Inst. Fourier (Grenoble) **51** (2001), no. 4, 903–937.

[BN05] ——— and ———, *On modified circular units and annihilation of real classes*, Nagoya Math. J. **177** (2005), 77–115.

[BO01] ——— et H. Oukhaba, *Sur la torsion de la distribution ordinaire universelle attachée à un corps de nombres*, Manuscripta Math. **106** (2001), no. 1, 117–130.

[Bru67] A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.

[BG03] D. Burns and C. Greither, *On the equivariant Tamagawa number conjecture for Tate motives*, Invent. Math. **153** (2003), no. 2, 303–359.

[Col79] R. F. Coleman, *Division values in local fields*, Invent. Math. **53** (1979), no. 2, 91–116.

[Col83] ———, *Local units modulo circular units*, Proc. Amer. Math. Soc. **89** (1983), no. 1, 1–7.

[Cor98] Pietro Cornacchia, *Fitting ideals of class groups in a $\mathbf{Z}_p$-extension*, Acta Arith. **87** (1998), no. 1, 79–88.

[Enn72] V. Ennola, *On relations between cyclotomic units*, J. Number Theory **4** (1972), 236–247.

[FGS81] L. J. Federer and B. H. Gross, *Regulators and Iwasawa modules*, Invent. Math. **62** (1981), no. 3, With an appendix by Warren Sinnott, pp . 443–457.

[FG04] Matthias Flach, *The equivariant Tamagawa number conjecture : a survey*, Stark's conjectures : recent work and new directions, Contemp. Math., vol. 358, Amer. Math. Soc., Providence, RI, 2004, With an appendix by C. Greither, pp. 79–125.

[Gil79] Roland Gillard, *Unités cyclotomiques, unités semi-locales et $\mathbf{Z}_\ell$-extensions*, Ann. Inst. Fourier (Grenoble) **29** (1979), no. 1, xiv, 49–79.

[GK89] Robert Gold and Jae Moon Kim, *Bases for cyclotomic units*, Compositio Math. **71** (1989), no. 1, 13–27.

[Gre92] Cornelius Greither, *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier (Grenoble) **42** (1992), no. 3, 449–499.

[Gre93] ———, *Über relativ-invariante Kreiseinheiten und Stickelberger--Elemente*, Manuscripta Math. **80** (1993), no. 1, 27–43.

[Iwa72] K. Iwasawa, *Lectures on p-adic L-functions*, Princeton University Press, Princeton, N.J., 1972, Annals of Mathematics Studies, No. 74.

[Jau94] Jean-François Jaulent, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 301–325.

[KNF96] M. Kolster, T. Nguyễn-Quang-Dỗ, and V. Fleckinger, *Twisted S-units, p-adic class number formulas, and the Lichtenbaum conjectures*, Duke Math. J. **84** (1996), no. 3, 679–717.

[KS95] James S. Kraft and René Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), no. 1-2, 135–155, Special issue in honour of Frans Oort.

[KN95] Radan Kučera and Jan Nekovář, *Cyclotomic units in $\mathbf{Z}_p$-extensions*, J. Algebra **171** (1995), no. 2, 457–472.

[Kuč03] Radan Kučera, *A note on circular units in $\mathbb{Z}_p$-extensions*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 223–229, XXIIèmes Journées Arithmétiques (Lille, 2001).

[Kuz72] L. V. Kuz′min, *The Tate module of algebraic number fields*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 267–327.

[Kuz96] ———, *On formulas for the class number of real abelian fields*, Izv. Ross. Akad. Nauk Ser. Mat. **60** (1996), no. 4, 43–110.

[LMN] M. Lescop, A. Movahhedi et T. Nguyễn-Quang-Dỗ, *Iwasawa descent and co-descent for units modulo circular units*, preprint (2005), with an appendix by J.-R. Belliard.

[Lan90] S. Lang, *Cyclotomic fields I and II*, second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, With an appendix by K. Rubin.

[MW84] B. Mazur and A. Wiles, *Class fields of abelian extensions of* **Q**, Invent. Math. **76** (1984), no. 2, 179–330.

[Ngu05] T. Nguyễn-Quang-Dỗ, *Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé*, preprint (2005).

[Oza97] M. Ozaki, *On the cyclotomic unit group and the ideal class group of a real abelian number field. I, II*, J. Number Theory **64** (1997), no. 2, 211–222, 223–232.

[Rub87] K. Rubin, *Global units and ideal class groups*, Invent. Math. **89** (1987), no. 3, 511–526.

[RW02] J. Ritter and A. Weiss, *The lifted root number conjecture and Iwasawa theory*, Mem. Amer. Math. Soc. **157** (2002), no. 748, viii+90.

[Sin80] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), no. 2, 181–234.

[Sol92] D. Solomon, *On a construction of p-units in abelian fields*, Invent. Math. **109** (1992), no. 2, 329–350.

[Tat84] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Progress in Mathematics, vol. 47, Birkhäuser Boston Inc., Boston, MA, 1984, Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

[Ta99] H. Taya,*On p-adic zeta functions and $\mathbb{Z}_p$-extensions of certain totally real number fields*, Tohoku Math. J. **51** (1999), no. 2, 21–33.

[Tsu99] T. Tsuji, *Semi-local units modulo cyclotomic units*, J. Number Theory **78** (1999), no. 1, 1–26.

[Tsu01] ———, *The Stickelberger elements and the cyclotomic units in the cyclotomic $\mathbb{Z}_p$-extensions*, J. Math. Sci. Univ. Tokyo **8** (2001), no. 2, 211–222.

[Was97] L. Washington, *Introduction to cyclotomic fields*, second ed., Springer-Verlag, New York, 1997.

[Wil90] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), no. 3, 493–540.

[Yin00] L. Yin, *Distributions on a global field*, J. Number Theory **80** (2000), no. 1, 154–167.