



HAL
open science

Indices isotypiques des éléments cyclotomiques.

Tatiana Beliaeva, Jean-Robert Belliard

► **To cite this version:**

Tatiana Beliaeva, Jean-Robert Belliard. Indices isotypiques des éléments cyclotomiques.. 2009. hal-00438674v1

HAL Id: hal-00438674

<https://hal.science/hal-00438674v1>

Preprint submitted on 4 Dec 2009 (v1), last revised 15 Dec 2011 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INDICES ISOTYPIQUES DES ÉLÉMENTS CYCLOTOMIQUES.

par

Tatiana Beliaeva & Jean-Robert Belliard

Résumé. — Given F a real abelian field, p an odd prime and χ any Dirichlet character of F we give a method for computing the χ -index $(H^1(G_S, \mathbb{Z}_p(r))^\chi : C^F(r)^\chi)$ where the Tate twist r is an odd integer $r \geq 3$, the group $C^F(r)$ is the group of higher circular units, G_S is the Galois group over F of the maximal S ramified algebraic extension of F , and S is the set of places of F dividing p . This χ -index can now be computed in terms only of elementary arithmetic of finite fields \mathbb{F}_ℓ . Our work generalizes previous results by Kurihara who used the assumption that the order of χ divides $p - 1$.

Table des matières

Introduction.....	1
1. Morphisme de descente explicite.....	3
2. Éléments cyclotomiques et relations de normes tordues.....	5
3. Caractères des représentations en jeu.....	8
4. Composantes isotypiques.....	10
5. Les morphismes de réduction modulo ℓ	11
6. Le thème d'indice.....	14
7. Image explicite des χ -éléments cyclotomiques.....	17
Références.....	21

Introduction

Soit F un corps de nombres abélien totalement réel, d'anneau d'entiers O_F , de groupe de Galois $G = \text{Gal}(F/\mathbb{Q})$ et $p \neq 2$ un nombre premier rationnel fixé dans toute la suite. On note $S = S(F)$ l'ensemble des places de F divisant p , on note Ω_S l'extension algébrique maximale non ramifiée hors de S de F et $G_S = \text{Gal}(\Omega_S/F)$. Les objets mathématiques centraux de cet article sont les groupes de cohomologie galoisienne $H^i(G_S, \mathbb{Z}_p(r)) = \varprojlim H^i(G_S, \mathbb{Z}/p^n(r))$, pour $r \in \mathbb{N}$, $r \geq 2$ et pour $i = 1$ ou 2 , vus comme $\mathbb{Z}_p[G]$ -modules. Ces groupes de cohomologie galoisienne sont connus pour être isomorphes aux groupes de cohomologie étale $H^i(\text{spec } O_F[1/p], \mathbb{Z}_p(r))$. Parmi les motivations leur étude il y a leur interprétation en K -théorie. Sous la conjecture de Quillen-Lichtenbaum ces groupes sont aussi isomorphes pour $r \geq 2$ aux p -adifs

$K_{2r-i}(O_F) \otimes \mathbb{Z}_p$ des groupes de K -thorie de Quillen (voir [17] pour la construction des groupes de K -thorie suprieurs). Cependant notre travail se situe entirement en cohomologie galoisienne p -adique et est donc logiquement independant de ce contexte conjectural. En arithmtique ces groupes s'interprtent comme des analogues suprieurs des groupes des p -units (pour $i = 1$ et $r \notin \{0, 1\}$) et des p -groupes de S -classes d'idaux (pour $i = 2$ et $r \geq 0$). Ces analogies sont prcises par une suite exacte due Kolster, Nguyễn-Quang-Dỗ et Fleckinger pour $i = 1$ (voir theorem 3.2 de [14] p.689) et une suite exacte due Kurihara pour $i = 2$ (voir lemma 4.3 de [15] p. 269). Ils sont aussi particulirement intressants tudier en liaison avec les valeurs spciales des fonctions L en $s = 1 - r$: ils sont au premier plan dans les dmonstrations des conjectures la Bloch-Kato pour les valeurs spciales des fonctions L motiviques dans le cas particuliers des fonctions L de Dirichlet (voir entre autres [5, 14, 4, 11, 6]).

Un des points culminants dans l'article [14] est une formule d'indice, consquence du theorem 5.4 de [14]

$$\# \left(\frac{H^1(G_S, \mathbb{Z}_p(r))}{C^F(r)} \right) = \# H^2(G_S, \mathbb{Z}_p(r))$$

valable dans cette version simplifie pour F totalement rel et r impair. Ici $C^F(r)$ (voir la dfinition 2.4) est l'analogue suprieur des units circulaires, et cette formule d'indice est donc l'analogue suprieur de la formule d'indice de Sinnott : une version algbrique de la formule analytique du nombre de classes de Dedekind. Cette formule d'indice passe aux χ -composantes, au moins lorsque $p \nmid [F : \mathbb{Q}]$, pour tout caractre χ sur $G = \text{Gal}(F/\mathbb{Q})$. Le principal rsultat de cet article est de presenter une mthode explicite et lmentaire pour calculer les χ -indices $(H^1(G_S, \mathbb{Z}_p(r))^\chi : C^F(r)^\chi)$ pour tous les caractres de Dirichlet χ (voir le thorme 6.1, son corollaire 6.7 et la formulation explicite du thorme 7.4). Ce travail doit normment Kurihara et s'inspire de son article [15]. Dans cet article Kurihara introduit une mthode remarquable pour calculer ces χ -indices en liaison avec l'ordre du $H^2(G_S, \mathbb{Z}_p(r))$, qu'il considre comme le p -adifi du groupe de Tate-Shafarevich associ au motif $h^0(\mathbb{Q}(\zeta_f))$. La mthode de Kurihara ramne le calcul de χ -indice de l'arithmtique dans des corps finis \mathbb{F}_ℓ , mais n'est compltement dcrite dans l'article [15] que pour les caractres de Dirichlet χ dont l'ordre divise $p - 1$. L'apport principal du present article est de se dispenser de cette hypothse restrictive. Pour ce faire on est parvenu remplacer les considrations sur l'ordre de certains lments spciaux dans [15] par des isomorphismes canoniques et gnraux de χ -composantes (voir le thorme 5.2).

Cet article est compos comme suit. Dans la section 1 on dfinit les notations $H^1(G_S, \mathbb{Z}_p(r))$ en justifiant les restrictions $r \geq 3$ impairs et F totalement rel. Puis on rappelle la construction d'un morphisme de descente classique (voir par exemple [14]) $\overline{U}'_\infty(r-1)_{G_\infty} \xrightarrow{\alpha} H^1(G_S, \mathbb{Z}_p(r)) \circ \overline{U}'_\infty$ dsigne la limite projective pour les normes des p -adifs des p -units des $F_n = F(\mu_{p^n})$ le long des tages finis de la tour $F_\infty = \bigcup_n F_n$ et o $G_\infty = \text{Gal}(F_\infty/F)$. Il s'agit surtout, pour l'usage ultrieur fait dans cet article, de prciser explicitement les images de p -units donnees.

Dans la section 2 on dfinit, en utilisant le morphisme α et suivant [14] et [15], les lments cyclotomiques en cohomologie galoisienne $c_b^F(r)$ qui engendrent le groupe

$C^F(r)$ et concident avec le p -adif des éléments cyclotomiques de Soul ([21] ou aussi [22]) si la conjecture de Quillen-Lichtenbaum est vraie. On étudie aussi les relations de normes reliant ces générateurs. Suivant le même esprit qu'en section 1 on précise explicitement les images de ces $c_b^F(r)$ par restriction et réduction modulo p^n dans $H^1(G_S(F_n), \mathbb{Z}/p^n(r))$.

Dans la section 3 on calcule le caractère commun (qui est le caractère régulier) des $G = \text{Gal}(F/\mathbb{Q})$ -représentations linéaires obtenues à partir de $C^F(r) \otimes \mathbb{Q}_p$, $H^1(G_S, \mathbb{Q}_p(r))$ et $\overline{U}'_\infty(r-1)_{G_\infty} \otimes \mathbb{Q}_p$. Pour ce faire nous utilisons l'injectivité et la finitude du conoyau de α démontré dans [14]; et la théorie de Coleman ([7]) pour calculer le caractère des unités semi-locales et en déduire celui des p -unités.

Dans la section 4 on regroupe les lemmes algébriques concernant les χ -parties qui servent à notre étude. Pour des descriptions plus complètes des propriétés fonctorielles des χ -parties et χ -quotients, le lecteur est invité à consulter [20], ou encore [23]. On indique aussi quel χ -indice précis est calculé dans la suite, parmi la multitude de nuances possibles lorsque $p \mid [F : \mathbb{Q}]$. Tant que faire se peut, on justifie le choix de χ -indice fait dans cet article.

Dans la section 5 on reprend la construction par Kurihara du morphisme $\phi_{\ell,n}$ de réduction modulo ℓ qui est au cœur de cette méthode de calcul des χ -indices. On détaille soigneusement une interprétation kummerienne de ce morphisme avec le diagramme-cl (12); et l'on démontre le théorème d'isomorphisme 5.2 qui est le point essentiel dans notre amélioration de l'approche de Kurihara.

Dans la section 6 on utilise le théorème 5.2 pour démontrer la formule d'indice du théorème 6.1 qui est le résultat principal de cet article. Par rapport à la démarche de [15], pour démontrer ce théorème il faut essentiellement dans cette section circonvenir les difficultés techniques supplémentaires occasionnées par l'éventualité $p \mid [F : \mathbb{Q}]$ (cas non semi-simple). C'est ici qu'interviennent à la fois les propriétés fonctorielles des χ -parties rappelés en section 4 et le gain conceptuel obtenu avec l'isomorphisme du théorème 5.2.

Dans la section 7 on précise l'énoncé du théorème 6.1 en donnant une formule explicite pour les images d'éléments cyclotomiques contre le morphisme $\phi_{\ell,n}$ de réduction modulo ℓ et en fixant des générateurs concrets des χ -parties considérées.

Remerciements : Les deux auteurs remercient Thong Nguyễn-Quang-Đỗ qui nous a suggéré ce sujet comme une collaboration possible.

1. Morphisme de descente explicite

On fixe un plongement de $\overline{\mathbb{Q}}$ dans \mathbb{C} . Ce plongement définit un système de racines de l'unité compatibles en posant $\zeta_n := e^{2i\pi/n}$, pour $n \in \mathbb{N}$, $n \geq 1$. On rappelle que F un corps de nombres abélien totalement réel, que $p \neq 2$ un nombre premier rationnel fixé dans toute la suite. Soit $S = S(F)$ l'ensemble de places de F au-dessus de p . On note Ω_S l'extension algébrique maximale de F non ramifiée hors S et $G_S = \text{Gal}(\Omega_S/F)$ son groupe de Galois. On note aussi $\mathcal{G}_S = \text{Gal}(\Omega_S/\mathbb{Q})$. Soit

$F_n = F(\zeta_{p^n}) \subset \Omega_S$. On note $G_S(F_n)$ le groupe $\text{Gal}(\Omega_S/F_n)$, on note $G_n = \text{Gal}(F_n/F)$ et $G_\infty = \text{Gal}(F_\infty/F) \cong \varprojlim G_n$, o $F_\infty = \bigcup_n F_n$.

La donne du systme compatible en norme ζ_{p^n} dfinit aussi un gnrateur $t(1)$ du module de Tate $\mathbb{Z}_p(1) := \varprojlim \mu_{p^n}$, o μ_m dsigne le groupe des racines de l'unit d'ordre divisant m dans $\overline{\mathbb{Q}}$. Pour tout entier $r \geq 1$ on note $t(r) \in \mathbb{Z}_p(r)$ la puissance tensorielle r^{ime} de $t(1)$ qui est un gnrateur de $\mathbb{Z}_p(r) := \mathbb{Z}_p(1)^{\otimes r}$ et pour tout entier $n \geq 1$ on note $t(r)_n$ la n^{ime} projection de $t(r)$ qui engendre $\mathbb{Z}/p^n(r)$. Si $\kappa: \mathcal{G}_S \rightarrow \mathbb{Z}_p^\times$ dsigne le "caractre" cyclotomique, alors l'action de \mathcal{G}_S sur $\mathbb{Z}_p(r)$ est donne par $\gamma(x) = \kappa(\gamma)^r x$. Ces conventions permettent de dfinir pour tout entier $r \geq 1$ et tout $\mathbb{Z}_p[\mathcal{G}_S]$ -module M son r^{ime} -tordu la Tate, not $M(r)$, par $M(r) := M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(r)$, le groupe \mathcal{G}_S agissant diagonalement. Il est parfois plus commode de voir $M(r)$ comme le p -groupe M lui-mme muni de l'action de \mathcal{G}_S tordue : $\gamma *_r x := \kappa(\gamma)^r \gamma(x)$. Le principal objet tudi dans cet article est le groupe de cohomologie galoisienne :

$$H^1(G_S, \mathbb{Z}_p(r)) := \varprojlim_n H^1(G_S, \mathbb{Z}/p^n(r)).$$

Suivant Kurihara ([15]) on va se limiter aux twists r impairs, un corps F totalement rel et supposer $r > 1$. Cette approche est base sur l'existence d'lments spciaux engendrant un sous- $\mathbb{Z}_p[G]$ -module libre de rang 1 et d'indice fini dans $H^1(G_S, \mathbb{Z}_p(r))$ (voir thorme 3.4). D'aprs les calculs de rang p. 223 de [13] la seule possibilit pour que $H^1(G_S, \mathbb{Z}_p(r))$ soit de \mathbb{Z}_p -rang gal l'ordre de $G = \text{Gal}(F/\mathbb{Q})$ est de prendre le corps F totalement rel et le twist $r > 1$ impair. Dans le cas du twist $r = 1$ on a $H^1(G_S, \mathbb{Z}_p(r)) \cong \overline{U}'_F := U'_F \otimes \mathbb{Z}_p$, la pro- p -compltion du groupe des S -units de F . Le twist $r = 1$ fait l'objet d'un nombre considrable de travaux, est connu pour tre techniquement plus difficile et ne sera pas abord dans cet article. L'un des avantages plus accessoires de ces restrictions en gnralit est le lemme suivant :

Lemme 1.1. — *On suppose $r > 1$ impair, F totalement rel et $p \neq 2$; alors le \mathbb{Z}_p -module $H^1(G_S, \mathbb{Z}_p(r))$ est sans torsion.*

Démonstration. — D'aprs le lemme 2.2 de [14] la torsion de $H^1(G_S, \mathbb{Z}_p(r))$ s'identifie $\mathbb{Q}_p/\mathbb{Z}_p(r)^{G_\infty}$. Comme F est totalement rel la conjugaison complexe τ est un lment bien dfini de G_∞ qui vrifie $\kappa(\tau)^r = (-1)^r = -1$ puisque r est impair. Cet lment agit donc simultanment par multiplication par 1 et -1 sur $\mathbb{Q}_p/\mathbb{Z}_p(r)^{G_\infty}$ ce qui dmontre que la torsion de $H^1(G_S, \mathbb{Z}_p(r))$ est annul par 2. \square

Dans la fin de section on redonne la construction et une formule explicite pour un morphisme de descente classique (voir [14] par exemple) :

$$\overline{U}'_\infty(r-1)_{G_\infty} \xrightarrow{\alpha} H^1(G_S, \mathbb{Z}_p(r)),$$

o \overline{U}'_∞ dsigne la limite projective relativement aux applications de norme des pro- p -compltions des S -units $\overline{U}'_n = \overline{U}'_{F_n}$ le long de l'extension F_∞/F .

Soit $u_\infty = (u_n)_{n \in \mathbb{N}}$ une suite cohrente en norme de \overline{U}'_∞ avec $u_n \in F_n$. Alors par le cocycle de Kummer $\overline{U}'_n/p^n \otimes \mathbb{Z}/p^n(r-1) \hookrightarrow H^1(G_S(F_n), \mathbb{Z}/p^n(r))$, chaque $u_n \otimes t(r-1)_n$ dfinit un lment $x_n \in H^1(G_S(F_n), \mathbb{Z}/p^n(r))$. Concrtement on a la

formule

$$x_n(g) = \frac{g(\sqrt[p^n]{u_n})}{\sqrt[p^n]{u_n}} \otimes t(r-1)_n \in \mu_{p^n}(r-1) \cong \mathbb{Z}/p^n(r).$$

Pour tout m on pose

$$\alpha_m(u_\infty \otimes t(r-1)) = \text{cor}_{F(\zeta_{p^m})/F}(x_m) \in H^1(G_S, \mathbb{Z}/p^m(r)).$$

La cohérence en norme des u_n impose alors que les $\alpha_m(u_\infty)$ forment une suite cohérente pour les applications $H^1(G_S, \mathbb{Z}/p^{m+k}(r)) \rightarrow H^1(G_S, \mathbb{Z}/p^m(r))$, qui définit donc un élément de $H^1(G_S, \mathbb{Z}_p(r))$. On obtient ainsi un morphisme de modules galoisiens $U'_\infty(r-1) \rightarrow H^1(G_S, \mathbb{Z}_p(r))$ et puisque l'action de G_∞ est triviale droite on obtient un morphisme $\alpha: \overline{U}'_\infty(r-1)_{G_\infty} \rightarrow H^1(G_S, \mathbb{Z}_p(r))$ caractérisé par les formules (pour tout $m \geq 1$ et tout $\overline{u_\infty \otimes t(r-1)} = \overline{(u_n)_{n \in \mathbb{N}} \otimes t(r-1)} \in \overline{U}'_\infty(r-1)_{G_\infty}$) :

$$(1) \quad (\varphi_m \circ \alpha)(\overline{u_\infty \otimes t(r-1)}) = \sum_{g \in G_m} (\kappa^{r-1}(g)gu_m) \otimes t(r-1)_m,$$

où l'on identifie $\overline{U}'_m \otimes \mathbb{Z}/p^m(r-1)$ avec son image dans $H^1(G_S(F_m), \mathbb{Z}/p^m(r))$ par l'homomorphisme de Kummer et où $\varphi_m: H^1(G_S, \mathbb{Z}_p(r)) \rightarrow H^1(G_S(F_m), \mathbb{Z}/p^m(r))$ est la composée des applications (commutantes) de réduction modulo p^m et de restriction. On doit aussi remarquer que par définition $G_m = \text{Gal}(F(\zeta_{p^m})/F)$ opère sur μ_{p^m} et en particulier $\kappa(g)$ est bien défini modulo p^m pour tout $g \in G_m$.

Proposition 1.2. — On note X'_∞ la limite de projective pour les applications de normes des p -parties des (p) -classes X'_n de F_n . Le morphisme α induit la suite exacte

$$(2) \quad 0 \longrightarrow (\overline{U}'_\infty(r-1))_{G_\infty} \xrightarrow{\alpha} H^1(G_S, \mathbb{Z}_p(r)) \longrightarrow X'_\infty(r-1)^{G_\infty} \longrightarrow 0.$$

Démonstration. — L'application α coïncide avec celle définie dans la preuve du théorème 3.2 bis ([14] p.691). \square

2. Éléments cyclotomiques et relations de normes tordues

Le conducteur de F est de la forme $f = p^a d$ avec $p \nmid d$. Pour tout $b \mid d$ et tout $n \geq a$ on note

$$\varepsilon_{b,n}^F = N_{\mathbb{Q}(\zeta_{bp^n})/F_n \cap \mathbb{Q}(\zeta_{bp^n})}(1 - \zeta_{bp^n}).$$

Pour $n \geq a$, les p -unités $\varepsilon_{b,n}^F$ sont cohérentes en norme suivant N_{F_{n+1}/F_n} et définissent donc des éléments locaux

$$\varepsilon_{b,\infty}^F = (\varepsilon_{b,n}^F)_{n \geq a} \in \overline{U}'_\infty.$$

Et pour obtenir la cohérence en normes pour tout n on convient de noter pour $n < a$:

$$\varepsilon_{b,n}^F = N_{F_a/F_n}(\varepsilon_{b,a}^F).$$

Si un nombre premier $\ell \neq p$ divise d et pas b alors il est non ramifié dans $\mathbb{Q}(\zeta_{bp^\infty})/\mathbb{Q}$ et le Frobenius Fr_ℓ qui agit sur toutes les racines de l'unité d'ordre premier ℓ par multiplication par ℓ est un élément bien défini de l'algèbre de groupe complète

$\mathbb{Z}_p[[\text{Gal}(\mathbb{Q}(\zeta_{b p^\infty}) \cap F_\infty/\mathbb{Q})]]$. Les lments cyclotomiques sont lis par les relations de normes bien connues (pour tout premier ℓ et tout entier b avec $\ell b \mid d$) :

$$(3) \quad N_{\mathbb{Q}(\zeta_{\ell b p^\infty}) \cap F_\infty / \mathbb{Q}(\zeta_{b p^\infty}) \cap F_\infty}(\varepsilon_{\ell b, \infty}^F) = \begin{cases} (1 - Fr_\ell^{-1})\varepsilon_{b, \infty}^F & \text{si } \ell \nmid b \\ \varepsilon_{b, \infty}^F & \text{sinon.} \end{cases}$$

Le personnage principal de notre tude est le codescendu du r -ime tordu de ces lments cyclotomiques.

Dfinition 2.1. — On appelle r -ime lment spcial p -adique de conducteur b et l'on note $c_b^F(r) \in H^1(G_S, \mathbb{Z}_p(r))$ l'image par α de $\overline{\varepsilon_{b, \infty}^F \otimes t(r-1)} \in (\overline{U}_\infty'(r-1))_{G_\infty}$:

$$(4) \quad c_b^F(r) := \alpha \left(\overline{\varepsilon_{b, \infty}^F \otimes t(r-1)} \right).$$

L'lment spcial attach F sur lequel on s'attardera plus particulirement est celui de conducteur d :

$$(5) \quad c^F(r) := c_d^F(r) = \alpha \left(\overline{\varepsilon_{d, \infty}^F \otimes t(r-1)} \right).$$

Ces lments spciaux sont caractriss par leurs images contre les morphismes $\varphi_m : H^1(G_S, \mathbb{Z}_p(r)) \rightarrow H^1(G_S(F_m), \mathbb{Z}/p^m(r))$.

Lemme 2.2. — Pour tout $b \mid d$ et tout $m \in \mathbb{N}$ on a :

$$(6) \quad \varphi_m(c_b^F(r)) = \sum_{g \in G_m} \kappa^{r-1}(g) g(\varepsilon_{b, m}^F) \otimes t(r-1)_m.$$

En particulier pour $m \geq a$ et pour tout $b \mid d$ on a :

$$(7) \quad \varphi_m(c_b^F(r)) = \sum_{g \in \text{Gal}(\mathbb{Q}(\zeta_{b p^m})/\mathbb{Q}(\zeta_{b p^a}) \cap F)} \kappa^{r-1}(g) g(1 - \zeta_{b p^m}) \otimes t(r-1)_m.$$

Démonstration. — Pour obtenir (6) il suffit d'appliquer la formule (1) la suite $(u_n) = \varepsilon_{b, \infty}$. Ici aussi les quantits $\kappa(g)$ sont bien dfinies modulo p^m parce que $\text{Gal}(\mathbb{Q}(\zeta_{b p^m})/\mathbb{Q})$ opre sur μ_{p^m} . Pour en dduire la formule (7) on reprend la dfinition $\varepsilon_{b, m}^F = N_{\mathbb{Q}(\zeta_{b p^m})/F_m \cap \mathbb{Q}(\zeta_{b p^m})}(1 - \zeta_{b p^m})$. Or $\text{Gal}(\mathbb{Q}(\zeta_{b p^m})/F_m \cap \mathbb{Q}(\zeta_{b p^m}))$ agit trivialement sur les racines p^m -imes de l'units et donc pour $h \in \text{Gal}(\mathbb{Q}(\zeta_{b p^m})/F_m \cap \mathbb{Q}(\zeta_{b p^m}))$ on a $\kappa^{r-1}(h) \equiv 1[p^m]$. Par identification de G_m avec $\text{Gal}(F_m \cap \mathbb{Q}(\zeta_{b p^m})/F \cap \mathbb{Q}(\zeta_{b p^m}))$ et par transitivit de la norme on obtient l'identit (7). \square

Remarque : Par construction mme, l'image dans $H^1(G_S(\mathbb{Q}(\zeta_f)), \mathbb{Z}_p(r))$ de l'lment spcial $c_b^F(r)$ est l'lment not $c_r(\zeta_f)$ et appel lment de Soul-Deligne dans la dfinition 3.1.2 de [11]. Pour les liens entre ces lments, ceux dfinis par Deligne dans [8], ceux dfinis par Soul dans la section 4.4 de [22] (voir aussi [21]), ceux dfinis par Beilinson dans [1], voir les articles originaux et les comparaisons faites dans [11] et [12].

Proposition 2.3. — Les r -imes lments spciaux de conducteurs diffrents sont lis par les relations de normes (pour tout nombre premier ℓ et tout b tel que $\ell b \mid d$) :

$$(8) \quad N_{\mathbb{Q}(\zeta_{\ell b p^\infty}) \cap F / \mathbb{Q}(\zeta_{b p^\infty}) \cap F}(c_{\ell b}^F(r)) = \begin{cases} (1 - \ell^{r-1} Fr_\ell^{-1})c_b^F(r) & \text{si } \ell \nmid b \\ c_b^F(r) & \text{sinon} \end{cases}$$

Démonstration. — On remarque tout d'abord que $\text{Gal}(\mathbb{Q}(\zeta_{\ell b p^\infty}) \cap F / \mathbb{Q}(\zeta_{b p^\infty}) \cap F)$ agit trivialement sur le module de Tate $\mathbb{Z}_p(r-1)$, tandis que, comme $\ell \neq p$, on a $Fr_\ell t(r-1) = \ell^{r-1}t(r-1)$. On part de la relation (3) qui après twist la Tate donne :

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{\ell b p^\infty}) \cap F / \mathbb{Q}(\zeta_{b p^\infty}) \cap F} (\varepsilon_{\ell b, \infty}^F \otimes t(r-1)) &= N_{\mathbb{Q}(\zeta_{\ell b p^\infty}) \cap F / \mathbb{Q}(\zeta_{b p^\infty}) \cap F} (\varepsilon_{\ell b, \infty}^F) \otimes t(r-1) \\ &= \begin{cases} ((1 - Fr_\ell^{-1})\varepsilon_{b, \infty}^F) \otimes t(r-1) & \text{si } \ell \nmid b \\ \varepsilon_{b, \infty}^F \otimes t(r-1) & \text{sinon.} \end{cases} \end{aligned}$$

Le cas particulier $\ell \mid b$ de la formule (8) s'en déduit alors immédiatement en prenant les co-invariants puis en appliquant α . Lorsque $\ell \nmid b$ on a :

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{\ell b p^\infty}) \cap F / \mathbb{Q}(\zeta_{b p^\infty}) \cap F} (\varepsilon_{\ell b, \infty}^F \otimes t(r-1)) &= ((1 - Fr_\ell^{-1})\varepsilon_{b, \infty}^F) \otimes t(r-1) \\ &= (\varepsilon_{b, \infty}^F \otimes t(r-1)) - (Fr_\ell^{-1}\varepsilon_{b, \infty}^F \otimes \ell^{r-1}Fr_\ell^{-1}t(r-1)) \\ &= (1 - \ell^{r-1}Fr_\ell^{-1})\varepsilon_{b, \infty}^F \otimes t(r-1). \end{aligned}$$

Et on conclut nouveau en prenant les co-invariants et en appliquant α . \square

Définition 2.4. — On appelle groupe des éléments cyclotomiques et on note $C^F(r)$ le sous-module de $H^1(G_S, \mathbb{Z}_p(r))$ engendré par les r -èmes éléments spéciaux de conducteurs divisant d :

$$C^F(r) = \langle c_b^F(r), b \mid d \rangle$$

L'un des intrants de ce groupe réside dans l'analogue supérieur de la formule analytique du nombre de classe démontré par Kolster, Nguyễn-Quang-Dỗ et Fleckinger. Par exemple on a l'égalité :

Théorème 2.5. — On rappelle que F est totalement réel et que $r \neq 1$ est impair.

$$\# \left(\frac{H^1(G_S, \mathbb{Z}_p(r))}{C^F(r)} \right) = \# H^2(G_S, \mathbb{Z}_p(r))$$

Démonstration. — C'est un cas particulier du théorème 5.4 p. 701 de [14] \square

La philosophie générale de la K -théorie arithmétique prédit que les $H^1(G_S, \mathbb{Z}_p(r))$ pour les r impairs se comportent comme des p -unités tordues, cette intuition tant précisée notamment par suite exacte (2) ; tandis que les $H^2(G_S, \mathbb{Z}_p(r))$ se comportent comme des p -groupes de S -classes d'idaux tordues, voir notamment le lemme 4.3 p. 269 de [15]. De ce point de vue l'égalité du théorème 2.5 est l'analogue supérieur et sans facteur parasite des formules d'indices de Sinnott pour le twist $r = 1$ ([18, 19]). La formule d'indice du théorème 2.5 passe aussi aux χ -composantes, au moins lorsque $p \nmid [F : \mathbb{Q}]$. Il est donc intéressant de trouver des méthodes de calcul explicite des ordres des χ -composantes du quotient $H^1(G_S, \mathbb{Z}_p(r)) / C^F(r)$ pour tous les caractères χ de F . C'est ce qui a été fait (parmi d'autres résultats) dans l'article [15] mais en supposant que l'exposant de G divise $p-1$, et en particulier que $p \nmid [F : \mathbb{Q}]$. Dans le cas général, que nous traitons ici, il faut aussi choisir une notion précise de χ -composantes. En effet au moins deux foncteurs naturels donnant des χ -composantes co-existent. On reviendra sur ces χ -composantes en section 4. Dans la section qui suit, pour mieux décrire les composantes qui vont nous intéresser, on calcule le caractère de quelques représentations linéaires.

3. Caractres des representations en jeu

Dfinition 3.1. — Soit G un groupe fini.

1. Pour tout $\mathbb{Z}_p[G]$ module M , on appelle caractre de M la fonction centrale sur G obtenue en prenant la trace de $M \otimes \mathbb{Q}_p$ vue comme representation de G .
2. On appelle caractre rgulier sur G le caractre de $\mathbb{Z}_p[G]$. On appelle caractre trivial sur G le caractre de \mathbb{Z}_p avec action triviale de G .

Il est bien connu que deux $\mathbb{Z}_p[G]$ -modules deviennent isomorphes aprs extension des scalaires de \mathbb{Z}_p \mathbb{Q}_p si et seulement si ils ont mme caractres.

Proposition 3.2. — On rappelle que le twist $r \neq 1$ est suppos impair et le corps de base F totalement rel.

1. $C^F(r)$ est d'indice fini dans $H^1(G_S, \mathbb{Z}_p(r))$.
2. $\alpha((\overline{U}'_\infty(r-1))_{G_\infty})$ est d'indice fini dans $H^1(G_S, \mathbb{Z}_p(r))$.
3. Le caractre commun sur $\text{Gal}(F/\mathbb{Q})$ des trois modules $C^F(r)$, $\alpha((\overline{U}'_\infty(r-1))_{G_\infty})$ et $H^1(G_S, \mathbb{Z}_p(r))$ est le caractre rgulier.

Démonstration. — 1– est une consquence du thorme 5.4 de [14] et 2– de la suite exacte (2). Pour 3– il suffit de calculer le caractre de $(\overline{U}'_\infty(r-1))_{G_\infty}$ par injectivité de α . Parce que r est impair et F totalement rel, ce caractre est le caractre rgulier, autrement dit $(\overline{U}'_\infty(r-1))_{G_\infty} \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[G]$. Ce rsultat fait probablement partie du folklore et par exemple est compatible avec les rangs mentionns dans [13]. Nous n'avons malheureusement pas trouv de rfrence qui prcise le caractre des modules qui nous concernent. Pour la commodité du lecteur on va noncer et refaire la preuve du lemme suivre qui conclut la démonstration de la proposition 3.2. \square

Lemme 3.3. — Soit \mathcal{U}_∞ (resp. $\overline{\mathcal{U}}_\infty$) la limite projective des units semi-locales (resp. globales) le long de la tour $F(\zeta_{p^\infty})/F$, relativement aux applications de norme.

1. Pour tout entier $r \neq -1$ le caractre de $\mathcal{U}_\infty(r)_{G_\infty}$ est le caractre rgulier. Le caractre de $\mathcal{U}_\infty(-1)_{G_\infty}$ est la somme du caractre rgulier et de celui de $\mathbb{Z}_p[S]$.
2. Si r est pair alors le module $\overline{\mathcal{U}}_\infty(r)_{G_\infty}$ est de caractre rgulier. Le caractre de $\overline{\mathcal{U}}_\infty(-1)_{G_\infty}$ est le caractre de \mathbb{Z}_p avec action triviale de G . Si r est impair et diffrent de -1 alors $\overline{\mathcal{U}}_\infty(r)_{G_\infty}$ est de \mathbb{Z}_p -torsion.
3. Les modules $\overline{\mathcal{U}}_\infty(r)_{G_\infty}$ et $\overline{\mathcal{U}}'_\infty(r)_{G_\infty}$ ont mme caractre.

Démonstration. — On note $\mathcal{G} = \text{Gal}(F_\infty/\mathbb{Q})$ et $\Lambda[\mathcal{G}]$ l'algbre de groupe pro- p -complt de \mathcal{G} . Clairement on a $\Lambda[\mathcal{G}] \cong \Lambda[\mathcal{G}](r)$ pour tout r . Lorsque p est modrment ramifi dans F , la thorie de Coleman donne une suite exacte (voir [10] ou [23] pour les dtails)

$$(9) \quad 0 \longrightarrow \bigoplus_{v|p} \mathbb{Z}_p(r+1) \longrightarrow \mathcal{U}_\infty(r) \longrightarrow \Lambda[\mathcal{G}] \longrightarrow \bigoplus_{v|p} \mathbb{Z}_p(r+1) \longrightarrow 0.$$

Sans aucune condition de ramification mais si F est ablien sur \mathbb{Q} il existe un sous-corps $L \subset F_\infty$ qui est ablien sur \mathbb{Q} , dans lequel p est modrment ramifi, et tel que $F(\zeta_{p^\infty}) = L(\zeta_{p^\infty})$ (voir par exemple [3] lemme 1.2). Ainsi la suite exacte (9) est valide pour tout corps F ablien.

On vrifie le cas $r = -1$ du 1- du lemme 3.3. Pour cela on note $\mathcal{V}_\infty(-1) \subset \Lambda[\mathcal{G}]$ l'image de $\mathcal{U}_\infty(-1)$. La suite (9) implique alors l'egalit $\mathcal{V}_\infty(-1)^{G_\infty} = 0$ et redonne par descente les deux suites exactes :

$$0 \longrightarrow \mathbb{Z}_p[S] \longrightarrow \mathcal{U}_\infty(-1)_{G_\infty} \longrightarrow \mathcal{V}_\infty(-1)_{G_\infty} \longrightarrow 0.$$

$$0 \longrightarrow \mathbb{Z}_p[S] \longrightarrow \mathcal{V}_\infty(-1)_{G_\infty} \longrightarrow \mathbb{Z}_p[G] \longrightarrow \mathbb{Z}_p[S] \longrightarrow 0.$$

Comme les caractres sont additifs en suites exactes cela dmontre la cas particulier $r = -1$ du point 1. Pour $r \neq -1$ les G_∞ invariants et co-invariants du module $\oplus_{v|p} \mathbb{Z}_p(r+1)$ sont finis et donc leur caractre est nul. La mme chasse au diagramme que ci-dessus mais en plus simple dmontre donc que $\mathcal{U}_\infty(r)_{G_\infty}$ et $\Lambda[\mathcal{G}]_{G_\infty}$ ont mme caractre, c'est--dire le caractre rgulier. Le point 1 est dmontr.

Pour 2 on sait, comme $p \neq 2$, que $\overline{U}_\infty \cong \mathbb{Z}_p(1) \oplus \overline{U}_\infty^+$. Si r est pair alors la conjugaison complexe de G_∞ agit trivialement sur $\mathbb{Z}_p(r)$ donc elle agit trivialement sur $\mathcal{U}_\infty^+(r)$ et agit par -1 sur $\mathcal{U}_\infty^-(r)$. On en dduit $\mathcal{U}_\infty(r)_{G_\infty} = (\mathcal{U}_\infty^+ \oplus \mathcal{U}_\infty^-)(r)_{G_\infty} = \mathcal{U}_\infty^+(r)_{G_\infty}$. Par la conjecture faible de Leopoldt, qui est un thorme pour l'extension cyclotomique, on sait que $\mathcal{U}_\infty^+/\overline{U}_\infty^+$ est un module de torsion de type fini sur l'algre d'Iwasawa classique $\Lambda = \Lambda[\text{Gal}(F_\infty/F(\zeta_p))]$. Donc $(\mathcal{U}_\infty^+/\overline{U}_\infty^+)(r)$ aussi et $(\mathcal{U}_\infty^+/\overline{U}_\infty^+)(r) \otimes \mathbb{Q}_p$ est de dimension finie sur \mathbb{Q}_p . En consequence les modules $(\mathcal{U}_\infty^+/\overline{U}_\infty^+)(r)^{G_\infty}$ et $(\mathcal{U}_\infty^+/\overline{U}_\infty^+)(r)_{G_\infty}$ ont mme caractre. Dans cette parit de r le point 2 se dduit donc du point 1 et de la suite exacte

$$0 \longrightarrow (\mathcal{U}_\infty^+/\overline{U}_\infty^+)(r)^{G_\infty} \longrightarrow \overline{U}_\infty^+(r)_{G_\infty} \longrightarrow \mathcal{U}_\infty^+(r)_{G_\infty} \longrightarrow (\mathcal{U}_\infty^+/\overline{U}_\infty^+)(r)_{G_\infty} \longrightarrow 0.$$

On passe au cas o r est impair. Comme F est totalement rel la conjugaison complexe est un lment bien dfini de G_∞ qui agit simultanment par -1 et par 1 sur $\overline{U}_\infty^+(r)_{G_\infty}$. Ce dernier module est donc trivial. Cela dmontre le cas r impair du point 2, puisque $\mathbb{Z}_p(r)_{G_\infty}$ a bien le caractre requis suivant $r = -1$ ou $r \neq -1$.

On dmontre le point 3. Les modules \overline{U}_∞ et \overline{U}'_∞ ont la mme Λ -torsion (savoir $\mathbb{Z}_p(1)$) et donc $\overline{U}'_\infty(r)$ et $\overline{U}_\infty(r)$ ont les mme G_∞ invariants (savoir 0 si $r \neq -1$ et $\mathbb{Z}_p(0)$ si $r = -1$.) En utilisant alors que $\overline{U}'_\infty(r)/\overline{U}_\infty(r)$ s'injecte dans $\mathbb{Z}_p[S](r)$ qui est de Λ -torsion on dmontre le point 3 en suivant le mme type de chasse au diagramme que prcdemment.

□

On nonce un premier rsultat utile notre calcul de χ -indice :

Thorme 3.4. — *L'lment spcial $c^F(r)$ engendre un sous- $\mathbb{Z}_p[G]$ -module libre de rang 1 de $H^1(G_S, \mathbb{Z}_p(r))$.*

Démonstration. — Comme on tudie le module monogne engendr par $c^F(r)$, il suffit de montrer que pour tout caractre de Dirichlet χ sur G l'lment $c^F(r) \otimes e_\chi \in C^F(r) \otimes \mathbb{C}_p$ est non nul, o e_χ dsigne l'idempotent usuel $e_\chi = (1/\#G) \sum_g \chi(g)g^{-1}$. On fixe χ un tel caractre, on note F_χ le sous-corps de F fix par $\text{Ker } \chi$ et on note kp^s le conducteur commun χ et F_χ (avec $s \leq a$). Le sous-espace χ -isotypique $C^F(r) \otimes e_\chi \subset C^F(r) \otimes \mathbb{C}_p$ est engendr par les $c_b^F(r) \otimes e_\chi$. Si $\mathbb{Q}(\zeta_{bp^\infty}) \cap F$ ne contient pas $\mathbb{Q}(\zeta_{kp^s}) \cap F$ alors $\mathbb{Q}(\zeta_{bp^\infty}) \cap F$ ne contient pas non plus F_χ parce que kp^s est le conducteur de χ . Et dans

ce cas $c_b^F(r) \otimes e_\chi$ est nul parce que tout lment non trivial g de $\text{Gal}(F_\chi/\mathbb{Q}(\zeta_{bp^\infty}) \cap F_\chi)$ agit simultanment par multiplication par 1 et par $\chi(g) \neq 1$ sur $c_b^F(r) \otimes e_\chi$. Par contre tous les $c_b^F(r) \otimes e_\chi$ pour tous les b tels que $\mathbb{Q}(\zeta_{bp^\infty})$ contienne F_χ sont colinaires $c_k^F(r) \otimes e_\chi$. En effet la formule (8) donne :

$$\begin{aligned} [\mathbb{Q}(\zeta_{bp^\infty}) \cap F : \mathbb{Q}(\zeta_{kp^\infty}) \cap F] c_b^F(r) \otimes e_\chi &= N_{\mathbb{Q}(\zeta_{bp^\infty}) \cap F / \mathbb{Q}(\zeta_{kp^\infty}) \cap F} (c_b^F(r) \otimes e_\chi) \\ &= \prod_{\ell|b, \ell \nmid k} (1 - \ell^{r-1} F r_\ell^{-1}) c_k^F(r) \otimes e_\chi, \end{aligned}$$

c'est--dire :

$$c_b^F(r) \otimes e_\chi = \frac{\prod_{\ell|b, \ell \nmid k} (1 - \ell^{r-1} \chi(\ell)^{-1})}{[\mathbb{Q}(\zeta_{bp^\infty}) \cap F : \mathbb{Q}(\zeta_{kp^\infty}) \cap F]} c_k^F(r) \otimes e_\chi.$$

Pour $r \neq 1$ les facteurs eulriens $(1 - \ell^{r-1} \chi(\ell)^{-1})$ ne s'annulent jamais et par la proposition 3.2 il suit $c_f^F(r) \otimes e_\chi \neq 0$. \square

4. Composantes isotypiques

Dans cette section on rappelle les dfinitions des χ -parties et χ -quotients et l'on dcrit prcisment quel χ -indice est calcul dans la suite en expliquant nos choix.

Dfinition 4.1. — Soit M un $\mathbb{Z}_p[G]$ -module et χ un caractre sur G . Suivant Tsuji [23], on note $\underline{\mathbb{Z}_p[\chi]}$ le $\mathbb{Z}_p[\chi]$ -module libre de rang 1 muni de l'action de G par multiplication par χ .

1. On appelle χ -partie de M et on note M^χ le plus grand sous-module de M sur lequel l'action de G est drite par χ . Formellement on peut dfinir M^χ par

$$\text{Hom}_{\mathbb{Z}_p[G]}(\underline{\mathbb{Z}_p[\chi]}, M) \cong M^\chi \subset M.$$

2. On appelle χ -quotient de M et on note M_χ le plus grand quotient de M sur lequel l'action de G est drite par χ . Formellement on peut dfinir M_χ par

$$M \twoheadrightarrow M_\chi \cong M \otimes_{\mathbb{Z}_p[G]} \underline{\mathbb{Z}_p[\chi]}.$$

Pour les propriets basiques de ces deux foncteurs on pourra consulter le §II de [20], la section 2 de [23], ou la thse du premier auteur [2]. Il serait beau d'avoir des mthodes simples pour calculer les ordres $\#(H^1(G_S, \mathbb{Z}_p(r))/C^F(r))^\chi$ ou $\#(H^1(G_S, \mathbb{Z}_p(r))/C^F(r))_\chi$ qui en gnral ne concident pas forcement. Dans la suite nous avons choisi de calculer $\#(H^1(G_S, \mathbb{Z}_p(r))^\chi / \langle c^F(r) \rangle^\chi)$, qui se prte le mieux notre mthode en raison du thorme 3.4. Trs souvent (en particulier par exemple si $p \nmid [F : \mathbb{Q}]$) tous ces χ -indices sont faux. Mais dans la gnralit avec laquelle cet article est rdig il semble utile d'expliquer ce choix. Dans le but d'tudier l'arithmtique des valeurs spciales d'une fonction L de Dirichlet (primitive) $L(s, \chi)$ il est naturel de fixer un caractre de Dirichlet χ de conducteur f , de prendre $F = F_\chi := \mathbb{Q}(\zeta_f)^{\text{Ker } \chi}$ et d'utiliser le module monogne engendr par l'lment cyclotomique $\langle c^F(r) \rangle$ la place du module $C^F(r)$. Dans cette restriction (naturelle) en gnralit, on a alors G cyclique, et notre choix n'est pas restrictif cause de la proposition suivante :

Proposition 4.2. — On suppose G cyclique.

1. Pour tout $\mathbb{Z}_p[G]$ -module fini M on a $\#M^x = \#M_\chi$, en particulier on a l'egalit

$$\# \left(\frac{H^1(G_S, \mathbb{Z}_p(r))}{\langle c^F(r) \rangle} \right)^x = \# \left(\frac{H^1(G_S, \mathbb{Z}_p(r))}{\langle c^F(r) \rangle} \right)_\chi.$$

2. On a un isomorphisme

$$\frac{H^1(G_S, \mathbb{Z}_p(r))^x}{\langle c^F(r) \rangle^x} \xrightarrow{\sim} \left(\frac{H^1(G_S, \mathbb{Z}_p(r))}{\langle c^F(r) \rangle} \right)_\chi^x.$$

Démonstration. — Lorsque G est cyclique engendr par g on a une suite exacte

$$0 \longrightarrow M^x \longrightarrow M \otimes \mathbb{Z}_p[\chi] \xrightarrow{g-\chi(g)} M \otimes \mathbb{Z}_p[\chi] \longrightarrow M_\chi \longrightarrow 0$$

Cela donne l'egalit des ordres du point 1.

Par le thorme 3.4 le module $\langle c^F(r) \rangle$ est isomorphe $\mathbb{Z}_p[G]$ et donc on a les isomorphismes $\langle c^F(r) \rangle_\chi \cong \mathbb{Z}_p[\chi] \cong \langle c^F(r) \rangle^x$. Par le lemme 2.2 de [23] on a une suite exacte longue :

$$0 \longrightarrow \langle c^F(r) \rangle^x \longrightarrow H^1(G_S, \mathbb{Z}_p(r))^x \longrightarrow \left(\frac{H^1(G_S, \mathbb{Z}_p(r))}{\langle c^F(r) \rangle} \right)_\chi^x \xrightarrow{\delta} \langle c^F(r) \rangle_\chi \longrightarrow \dots$$

Mais le module $\langle c^F(r) \rangle_\chi$ est sans \mathbb{Z}_p -torsion tandis que $(H^1(G_S, \mathbb{Z}_p(r))/\langle c^F(r) \rangle)_\chi^x$ est fini. Donc la flche de connexion δ est triviale et cela donne l'isomorphisme du point 2. \square

Comme cela ne presente pas de difficults supplémentaires, dans la suite on prend F ablien totalement rel quelconque, on prend χ un caractre sur G quelconque et l'on va calculer l'indice $\#(H^1(G_S, \mathbb{Z}_p(r))^x/\langle c^F(r) \rangle^x)$ en utilisant les morphismes de rduction modulo ℓ dans le style de Kurihara [15].

5. Les morphismes de rduction modulo ℓ

Soit un entier $n \geq 1$ et tant donn un nombre premier $\ell \in \mathbb{Z}$, tel que $\ell \equiv 1[dp^n]$, et un idal fix λ de F divisant ℓ , l'objet de cette section est de construire explicitement et de decire des propriets d'une application de rduction G -quivariante :

$$(10) \quad \phi_{\ell,n}: H^1(G_S, \mathbb{Z}/p^n(r)) \longrightarrow \bigoplus_{g \in G} H^1(\mathbb{F}_{\lambda^g}, \mathbb{Z}/p^n(r))$$

o \mathbb{F}_λ dsigne le corps rsiduel $O_F/\lambda \cong \mathbb{F}_\ell$. Cette application $\phi_{\ell,n}$ est essentiellement "l'application naturelle" de [15] p. 265, mais pour l'usage ulterieur fait dans cet article on l'examine un peu plus en dtail ici. Dans l'article [9] Gajda examine aussi une application naturelle en K -thorie $\phi_{p,l}: K_{2n+1}(\mathbb{Z}) \longrightarrow K_{2n+1}(\mathbb{F}_p)[l^\infty]$. Sous la conjecture de Quillen-Lichtenbaum, via les classes de Chern, le $\phi_{l,p}$ de Gajda donne ainsi une application naturelle de rduction pour le cas particulier o le corps F est un sous-corps de $\mathbb{Q}(\zeta_p)$. En supposant l'hypothse de Vandiver, Gajda dmontre que son $\phi_{l,p}$ est non nul pour un ensemble de premiers p dont il calcule la densit. Notre dmarche requiert des informations plus prcises que la non trivialit des $\phi_{\ell,n}$ et se situe en cohomologie Galoisienne.

On rappelle que \mathcal{G}_S dsigne $\text{Gal}(\Omega_S/\mathbb{Q})$. Pour tout idal premier λ de O_F divisant $\ell \equiv 1[dp]$, on se donne un idal $\mathcal{L} = \mathcal{L}(\lambda)$ de Ω_S divisant λ . Soit $D_{\mathcal{L}} \subset G_S$ le sous-groupe de dcomposition dans \mathcal{G}_S de \mathcal{L} . Alors pour tout p -groupe discret M muni d'une action continue de \mathcal{G}_S on a un morphisme de restriction $res_{\lambda}: H^1(G_S, M) \longrightarrow H^1(D_{\mathcal{L}}, M)$. Si $\sigma \in \mathcal{G}_S$ alors cette restriction commute avec le morphisme de conjugaison σ_* qui dfini l'action de σ sur les $H^1(H, M)$ pour tout sous-groupe ferm H de \mathcal{G}_S (voir par exemple [16] p. 44). Ainsi modulo l'identification $D_{\mathcal{L}} \stackrel{\sigma}{\cong} D_{\mathcal{L}^\sigma}$ ce morphisme de restriction dpend seulement de λ et pas du choix de \mathcal{L} divisant λ , parce qu'un autre choix conjugue \mathcal{L} par un $\sigma \in G_S$ qui agit trivialement sur $H^1(G_S, M)$. Par contre pour un $\sigma \in \mathcal{G}_S$ quelconque qui dfini un idal λ^σ de F divisant ℓ on a un diagramme commutatif

$$(11) \quad \begin{array}{ccc} H^1(G_S, M) & \xrightarrow{res_{\lambda}} & H^1(D_{\mathcal{L}}, M) \\ \downarrow \sigma_* & & \downarrow \sigma_* \\ H^1(G_S, M) & \xrightarrow{res_{\lambda^\sigma}} & H^1(D_{\mathcal{L}^\sigma}, M). \end{array}$$

Si $\lambda \notin S$, alors λ est non ramifi dans Ω_S et le pro- p -quotient maximal de $D_{\mathcal{L}}$ s'identifie avec le pro- p -quotient maximal de $\text{Gal}(\overline{\mathbb{F}}_{\ell}/\mathbb{F}_{\lambda})$. Donc pour tout p -groupe discret M on a des isomorphismes $H^1(D_{\mathcal{L}^\sigma}, M) \cong H^1(\mathbb{F}_{\lambda^\sigma}, M)$. Ceci pos on construit un morphisme $\phi_{\ell, n}$ comme annonc dans le diagramme (10) en prenant $M = \mathbb{Z}/p^n(r)$ dans ce qui prcde et en posant

$$\phi_{\ell, n} = \bigoplus_{g \in G} res_{\lambda^g}.$$

On obtient alors immdiatement que $\phi_{\ell, n}$ est G -quivariant pour l'action par permutation de G sur la somme directe $\bigoplus_{g \in G} H^1(\mathbb{F}_{\lambda^g}, \mathbb{Z}/p^n(r))$.

Pour rendre plus explicite cette application $\phi_{\ell, n}$ on va en donner une interpration kummerienne.

Dfnition 5.1. — Soit $\lambda \subset O_F$ divisant $\ell \equiv 1[dp^n]$, $\ell \neq 2$ un nombre premier et \mathcal{L} le premier fix de Ω_S divisant λ . Par abus on crit encore \mathcal{L} pour $\mathcal{L} \cap F_n$, et on identifie O_{F_n}/\mathcal{L} avec \mathbb{F}_{λ} .

1. On note $red_{\lambda}: F_n^{\times}/p^n \longrightarrow \mathbb{F}_{\lambda}^{\times}/p^n$ l'unique morphisme de groupe qui fasse commuter le diagramme

$$\begin{array}{ccccccc} F_n^{\times} & \longrightarrow & F_{n, \mathcal{L}}^{\times} & \xrightarrow{\sim} & \mathbb{F}_{\lambda}^{\times} \times (1 + \ell)^{\mathbb{Z}_{\ell}} \times \ell^{\mathbb{Z}} & \longrightarrow & \mathbb{F}_{\lambda}^{\times} \\ \downarrow & & & & & & \downarrow \\ F_n^{\times}/p^n & \xrightarrow{\quad red_{\lambda} \quad} & & & & & \mathbb{F}_{\lambda}^{\times}/p^n \end{array}$$

Explicitement red_{λ} associe la classe modulo les puissances p^n -imes de $x \in F_n^{\times}$ la classe modulo \mathcal{L} et les puissances p^n -imes de $x\ell^{-v_{\mathcal{L}}(x)}$.

2. Pour $r \geq 0$ on note $red_{\lambda}(r): F_n^{\times}/p^n(r) \longrightarrow \mathbb{F}_{\lambda}^{\times}/p^n(r)$ le r -ieme tordu de red_{λ} . Explicitement $red_{\lambda}(r)$ envoie $\bar{x} \otimes t(r)_n$ sur $(x\ell^{-v_{\mathcal{L}}(x)} + \mathcal{L}) \otimes t(r)_n$.

Cette d'finition permet de calculer explicitement les images de res_λ en utilisant le diagramme commutatif suivant :

$$(12) \quad \begin{array}{ccc} (F_n^\times/p^n)(r-1) & \xrightarrow{\quad red_{\lambda(r-1)} \quad} & (\mathbb{F}_\lambda^\times/p^n)(r-1) \\ \uparrow \wr & & \downarrow \wr \\ \{x \in F_n^\times/p^n; \forall v \nmid p, v(x) \equiv 0[p^n]\}(r-1) & \longrightarrow & (\mathbb{F}_\lambda^\times/p^n)(r-1) \\ \downarrow \wr & & \downarrow \wr \\ H^1(G_S(F_n), \mathbb{Z}/p^n(1))(r-1) & \longrightarrow & H^1(D_\mathcal{L}, \mathbb{Z}/p^n(1))(r-1) \\ \uparrow & \nearrow_{res_\lambda} & \\ H^1(G_S, \mathbb{Z}/p^n(r)) & & \end{array}$$

Les applications du triangle du bas sont des restrictions ; les deux triangles commutent de faon tautologique. Les isomorphismes verticaux s'obtiennent en utilisant le cocycle de Kummer. La commutativit du carr central est un simple jeu d'criture partir de ce cocycle (et il suffit de vrifier cette commutativit pour $r = 1$).

Le rsultat principal de cette section est le thorme d'isomorphisme suivant qui permet d'utiliser les morphismes de rduction pour calculer les χ -indices :

Thorme 5.2. — *Soit χ un caractre de $\text{Gal}(F/\mathbb{Q})$. Rappelons que f , le conducteur de F , vaut $f = dp^a$ avec $p \nmid d$. Prenons un $n > a$. Il existe un (une infinit de) nombre(s) premier(s) $\ell \equiv 1[dp^n]$ tel(s) que le morphisme $\phi_{\ell,n}$ induise un isomorphisme entre les χ -parties :*

$$H^1(G_S, \mathbb{Z}_p(r))^\chi/p^n H^1(G_S, \mathbb{Z}_p(r))^\chi \xrightarrow{\sim} \left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times/p^n(r-1) \right)^\chi.$$

D'monstration. — Tout d'abord les deux modules sont finis, isomorphes sur $\mathbb{Z}_p[G]$ $\mathbb{Z}_p[\chi]/p^n$. Pour $H^1(G_S, \mathbb{Z}_p(r))$ c'est parce qu'il est sans \mathbb{Z}_p -torsion (lemme 1.1) et de caractre rgulier (proposition 3.2) ; et donc la χ -partie $H^1(G_S, \mathbb{Z}_p(r))^\chi$ est un $\mathbb{Z}_p[\chi]$ -module sans torsion de rang 1. Pour le module de droite $\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times/p^n(r-1) \right)^\chi \cong (\mathbb{Z}/p^n[G])^\chi$, c'est vident. Il suffit donc de trouver un (une infinit de) ℓ tels que l'application

$$H^1(G_S, \mathbb{Z}_p(r))^\chi/p^n H^1(G_S, \mathbb{Z}_p(r))^\chi \longrightarrow \left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times/p^n(r-1) \right)^\chi$$

dduite de $\phi_{\ell,n}$ soit injective. On a une suite d'injection :

$$H^1(G_S, \mathbb{Z}_p(r))/p^n \xrightarrow{(1)} H^1(G_S, \mathbb{Z}/p^n(r)) \xrightarrow{(2)} H^1(G_S(F_n), \mathbb{Z}/p^n(r)) \xrightarrow{(3)} F_n^\times/p^n(r-1).$$

L'injectivit du morphisme (1) suit de la cohomologie de la suite

$$0 \longrightarrow \mathbb{Z}_p(r) \xrightarrow{p^n} \mathbb{Z}_p(r) \longrightarrow \mathbb{Z}/p^n(r) \longrightarrow 0.$$

L'injectivit du morphisme (2) suit par la suite d'inflation restriction grce la $\text{Gal}(F_n/F)$ -trivialit cohomologique des $\mathbb{Z}/p^n(r)$ pour $r \neq 0$ (lemme de Tate). L'injectivit du morphisme (3) vient de la thorie de Kummer et a dj t affirme dans

le diagramme (12). Soit \mathbb{L}_n l'ensemble des premiers rationnels $\ell \equiv 1[dp^n]$ et tels que $p^{n+1} \nmid (\ell - 1)$. Par le thorme de Dirichlet \mathbb{L}_n est infini. On considre l'application de rduction $red(r - 1)$ produit des $red_\lambda(r - 1)$ pour λ parcourant les premiers de F divisant les $\ell \in \mathbb{L}_n$:

$$red(r - 1): F_n^\times/p^n(r - 1) \longrightarrow \prod_{\ell \in \mathbb{L}_n} \left(\prod_{\lambda|\ell, \lambda \subset F} \mathbb{F}_\lambda^\times/p^n(r - 1) \right)$$

Lemme 5.3. — *Le morphisme $red(r - 1)$ est injectif.*

Démonstration. — Le foncteur $\otimes \mathbb{Z}/p^n(r - 1)$ est exact sur les \mathbb{Z}/p^n -modules, il suffit donc de vrifier cette injectivit pour $r = 1$. Soit $\varphi: F_n^\times \longrightarrow \prod_{\ell \in \mathbb{L}_n} \left(\prod_{\lambda|\ell, \lambda \subset F} \mathbb{F}_\lambda^\times \right)$ l'application de rduction avant de prendre le quotient modulo p^n . Si x est dans le noyau de φ alors $(x - 1)$ appartient tous les \mathcal{L} avec $v_{\mathcal{L}}(x) = 0$ soit une infinit d'idaux premiers distincts, et donc $x = 1$. Cela montre l'injectivit de φ . On en dduit un morphisme injectif

$$\iota: F_n^\times/p^n \longrightarrow \left(\prod_{\ell \in \mathbb{L}_n} \prod_{\lambda|\ell, \lambda \subset F} \mathbb{F}_\lambda^\times \right) / \varphi(p^n F_n^\times).$$

L'image de ι est contenu dans les lments d'ordre une puissance de p du quotient de droite. Ce sous-groupe des lments d'ordre une puissance de p s'injecte lui-mme naturellement dans $\prod_{\ell \in \mathbb{L}_n} \left(\prod_{\lambda|\ell, \lambda \subset F} \mathbb{F}_\lambda^\times/p^n \right)$ parce que p^n divise exactement l'ordre $\ell - 1$ des $\mathbb{F}_\lambda^\times$, pour $\ell \in \mathbb{L}_n$. \square

On reprend la preuve du thorme 5.2. Par exactitude gauche du foncteur χ -parties on dduit de ce qui prcde une suite de morphismes injectifs :

$$H^1(G_S, \mathbb{Z}_p(r))^{\chi}/p^n \hookrightarrow (H^1(G_S, \mathbb{Z}_p(r))/p^n)^{\chi} \hookrightarrow \prod_{\ell \in \mathbb{L}_n} \left(\prod_{\lambda|\ell, \lambda \subset F_n} \mathbb{F}_\lambda^\times/p^n(r - 1) \right)^{\chi}.$$

Pour un ℓ fix, l'application dduite par χ -partie de $\phi_{\ell, n}$ est la compose de cette suite d'injection avec la projection sur $\left(\prod_{\lambda|\ell, \lambda \subset F_n} \mathbb{F}_\lambda^\times/p^n(r - 1) \right)^{\chi}$: c'est une consquence de la commutativit du diagramme (12) (compatibilit entre res_λ et $red_\lambda(r - 1)$). Fixons x un $\mathbb{Z}_p[\chi]$ -gnrateur du $\mathbb{Z}_p[\chi]$ -module libre $H^1(G_S, \mathbb{Z}_p(r))^{\chi}$. Alors l'image de x dans $H^1(G_S, \mathbb{Z}_p(r))^{\chi}/p^n$ et donc aussi dans $\prod_{\ell \in \mathbb{L}_n} \left(\prod_{\lambda|\ell, \lambda \subset F_n} \mathbb{F}_\lambda^\times/p^n(r - 1) \right)^{\chi}$ engendre un module libre de rang 1 sur $\mathbb{Z}_p[\chi]/p^n$. Il en est forcment de mme pour (une infinit) des projections $\phi_{\ell, n}^\chi(x)$: cela dmontre le thorme 5.2. \square

6. Le thorme d'indice

Soit $n \in \mathbb{N}$ et ℓ un nombre premier tel que dp^n divise $\ell - 1$. Soit χ un caractre sur G . Dans la section 5 on a tudi le morphisme

$$\phi_{\ell, n}^\chi: H^1(G_S, \mathbb{Z}_p(r))^{\chi}/p^n H^1(G_S, \mathbb{Z}_p(r))^{\chi} \longrightarrow \left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times/p^n(r - 1) \right)^{\chi}.$$

Pour n fix on note \mathbb{L}'_n l'ensemble des premiers rationnels $\ell \equiv 1[dp^n]$. Le principal resultat original de cet article est le thorme d'indice suivant :

Thorme 6.1. —

$$\# \left(\frac{H^1(G_S, \mathbb{Z}_p(r))^x}{\langle c^F(r) \rangle^x} \right) = \max_{n \in \mathbb{N}} \left(\min_{\ell \in \mathbb{L}'_n} \left(\# \frac{\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1) \right)^x}{\phi_{\ell,n}^x(\langle c^F(r) \rangle^x)} \right) \right)$$

Dans la section 7 on dcrira concrtement le module $\phi_{\ell,n}^x(\langle c^F(r) \rangle^x)$, ce qui permettra de reformuler le thorme 6.1 de faon plus explicite. La suite de cette section est consacree la dmonstration de ce thorme 6.1, qui passe par quelques noncs intermdiaires intressants en eux-mmes. On commence par introduire des abrviations commodes.

Dfinition 6.2. — *On rappelle que F est ablien totalement rel de conducteur $p^a d$ avec $p \nmid d$.*

1. Par le thorme 5.2, si $n > a$ alors il existe une infinit de premiers $\ell \in \mathbb{L}'_n$ tels que le morphisme $\phi_{\ell,n}^x$ soit un isomorphisme. On notera $\mathbb{L}_n^{\text{iso}}$ cet ensemble de premiers rationnels.
2. On note $C_{F,r}^x$ le $\mathbb{Z}_p[\chi]$ -module libre $C_{F,r}^x = \langle c^F(r) \rangle^x$.
3. On note $H_{S,r}^x$ le $\mathbb{Z}_p[\chi]$ -module libre $H_{S,r}^x = H^1(G_S, \mathbb{Z}_p(r))^x$.

Avec ces notations on a la relation d'indice :

Lemme 6.3. — *Soit $n \in \mathbb{N}$ et $\ell \in \mathbb{L}'_n$. Alors*

$$\# \frac{H_{S,r}^x / p^n H_{S,r}^x}{C_{F,r}^x / (C_{F,r}^x \cap p^n H_{S,r}^x)} \leq \# \frac{\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1) \right)^x}{\phi_{\ell,n}^x(C_{F,r}^x / (C_{F,r}^x \cap p^n H_{S,r}^x))}.$$

Dmonstration. — On avait dj fait remarquer que les modules finis $H_{S,r}^x / p^n$ et $(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1))^x$ sont tous deux isomorphes $\mathbb{Z}_p[\chi] / p^n$ donc en particulier ils ont mme ordre. Le lemme se ramne donc l'ingalit vidente

$$\# \phi_{\ell,n}^x(C_{F,r}^x / (C_{F,r}^x \cap p^n H_{S,r}^x)) \leq \# C_{F,r}^x / (C_{F,r}^x \cap p^n H_{S,r}^x).$$

□

L'ingalit du lemme 6.3 conduit l'galit avec le \min du thorme 6.1. Il suffit juste d'observer que ce \min est actuellement atteint. C'est l'objet du second lemme intermdiaire qui est une consquence immdiate du thorme 5.2 :

Lemme 6.4. — *Soit $n \in \mathbb{N}$.*

1. Si $\ell \in \mathbb{L}_n^{\text{iso}}$ alors l'isomorphisme $\phi_{\ell,n}^x$ induit un isomorphisme :

$$\frac{H_{S,r}^x / p^n H_{S,r}^x}{C_{F,r}^x / (C_{F,r}^x \cap p^n H_{S,r}^x)} \xrightarrow{\sim} \frac{\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1) \right)^x}{\phi_{\ell,n}^x(C_{F,r}^x / (C_{F,r}^x \cap p^n H_{S,r}^x))}.$$

2. Pour tout $\ell \in \mathbb{L}_n^{\text{iso}}$ l'ingalit d'ordre du lemme 6.3 est une galit.

3. Si en outre n est tel que $p^n H_{S,r}^\chi \subset C_{F,r}^\chi$ et $\ell \in \mathbb{L}_n^{\text{iso}}$ alors $\phi_{\ell,n}^\chi$ induit un isomorphisme :

$$\frac{H_{S,r}^\chi}{C_{F,r}^\chi} \xrightarrow{\sim} \frac{\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda_g}^\chi / p^n(r-1) \right)^\chi}{\phi_{\ell,n}^\chi(C_{F,r}^\chi)}.$$

Démonstration. — Par définition même de $\mathbb{L}_n^{\text{iso}}$ si $\ell \in \mathbb{L}_n^{\text{iso}}$ alors l'homomorphisme

$$\phi_{\ell,n}^\chi : H_{S,r}^\chi / p^n \longrightarrow \left(\bigoplus_{g \in G} \mathbb{F}_{\lambda_g}^\chi / p^n(r-1) \right)^\chi$$

est un isomorphisme. On déduit l'isomorphisme du point 1 en passant au quotient gauche par $C_{F,r}^\chi / (C_{F,r}^\chi \cap H_{S,r}^\chi)$ et droite par son image. Le point 2 est une conséquence directe du point 1. Pour démontrer le point 3, partir des égalités $C_{F,r}^\chi \cap p^n H_{S,r}^\chi = p^n H_{S,r}^\chi$ et $C_{F,r}^\chi + p^n H_{S,r}^\chi = C_{F,r}^\chi$, il suffit d'observer les isomorphismes évidents :

$$\frac{H_{S,r}^\chi}{C_{F,r}^\chi} \cong \frac{H_{S,r}^\chi}{C_{F,r}^\chi + p^n H_{S,r}^\chi} \cong \frac{H_{S,r}^\chi / p^n H_{S,r}^\chi}{C_{F,r}^\chi / p^n H_{S,r}^\chi} \cong \frac{H_{S,r}^\chi / p^n H_{S,r}^\chi}{C_{F,r}^\chi / (C_{F,r}^\chi \cap p^n H_{S,r}^\chi)}.$$

□

On peut noncer le thorme ci-dessous qui permet de calculer résiduellement l'approximation modulo p^n du χ -indice du thorme 6.1 :

Thorme 6.5. — Pour tout $n \in \mathbb{N}$ on a l'égalité

$$\# \frac{H_{S,r}^\chi / p^n H_{S,r}^\chi}{C_{F,r}^\chi / (C_{F,r}^\chi \cap p^n H_{S,r}^\chi)} = \min_{\ell \in \mathbb{L}_n'} \left(\# \frac{\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda_g}^\chi / p^n(r-1) \right)^\chi}{\phi_{\ell,n}^\chi(\langle c^F(r) \rangle^\chi)} \right)$$

Démonstration. — Il suffit de combiner le lemme 6.3 avec le point 2 du lemme 6.4. □

On démontre maintenant le thorme 6.1.

Démonstration. — Comme $H_{S,r}^\chi$ est libre de rang 1 sur $\mathbb{Z}_p[\chi]$ qui est un anneau local, on a forcément :

- soit $C_{F,r}^\chi \subset p^n H_{S,r}^\chi$, ce qui a lieu pour $n = 0$ et devient faux dès que n est suffisamment grand.
- soit $p^n H_{S,r}^\chi \subset C_{F,r}^\chi$, ce qui a lieu dès que $n \geq N$ pour un certain N .

Cela tant, tant que $n < N$ l'approximation modulo p^n ne donne aucune information puisque :

$$\frac{H_{S,r}^\chi / p^n H_{S,r}^\chi}{C_{F,r}^\chi / (C_{F,r}^\chi \cap p^n H_{S,r}^\chi)} \cong H_{S,r}^\chi / p^n H_{S,r}^\chi \cong \mathbb{Z}_p[\chi] / p^n.$$

Par contre dès que $n \geq N$ alors l'approximation modulo p^n est exacte car on a :

$$\frac{H_{S,r}^\chi / p^n H_{S,r}^\chi}{C_{F,r}^\chi / (C_{F,r}^\chi \cap p^n H_{S,r}^\chi)} \cong \frac{H_{S,r}^\chi / p^n H_{S,r}^\chi}{C_{F,r}^\chi / p^n H_{S,r}^\chi} \cong \frac{H_{S,r}^\chi}{C_{F,r}^\chi}$$

De plus dès que $n > N$ on aura

$$\# \frac{H_{S,r}^\chi / p^n H_{S,r}^\chi}{C_{F,r}^\chi / (C_{F,r}^\chi \cap p^n H_{S,r}^\chi)} < \# \mathbb{Z}_p[\chi] / p^n.$$

Cela explique le $\max_{n \in \mathbb{N}}$ dans la formule du thorme 6.1 et conclut sa dmonstration compte-tenu du thorme 6.5. \square

Une autre faon, peut-tre plus propice aux approches numriques, de formuler le thorme 6.1 consiste se restreindre aux premiers rationnels $\ell \in \mathbb{L}'_1$ et tel que pour au moins un $n \leq v_p(\ell - 1)$, le χ -indice rsiduel $\# \frac{\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1)\right)^\chi}{\phi_{\ell,n}^\chi(\langle c^F(r) \rangle^\chi)}$, soit strictement infrieur l'indice maximal $\#\mathbb{Z}_p[\chi]/p^n$. C'est une faon de comprendre l'introduction d'indices toils par exemple p.261 de [15]. De ce point de vue, on peut viter le \max_n du thorme 6.1. Pour cela on dfinit d'abord des notations supplémentaires :

Dfnition 6.6. — *On rappelle que \mathbb{L}'_1 dsigne l'ensemble des premiers rationnels $\ell \equiv 1[dp]$.*

1. Pour tout $\ell \in \mathbb{L}'_1$ et tout $n \leq v_p(\ell - 1)$ on note $\text{ire}_{r,\chi,\ell,n}$ (pour indice rsiduel) la quantit :

$$\text{ire}_{r,\chi,\ell,n} := \# \frac{\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1)\right)^\chi}{\phi_{\ell,n}^\chi(\langle c^F(r) \rangle^\chi)}.$$

2. Pour tout n on note $\text{ima}_{\chi,n}$ (pour indice maximal) la quantit :

$$\text{ima}_{\chi,n} := \# \frac{\mathbb{Z}_p[\chi]}{p^n \mathbb{Z}_p[\chi]}.$$

Avec ces notations, pour remplacer le maximin du thorme 6.1 par un simple min, il suffit d'carter les cas d'galit entre indice rsiduel et indice maximal. Cela conduit au corollaire :

Corollaire 6.7. —

$$\# \frac{H^1(G_S, \mathbb{Z}_p(r))^\chi}{\langle c^F(r) \rangle^\chi} = \min_{\ell \in \mathbb{L}'_1, n \leq v_p(\ell-1)} \{ \text{ire}_{r,\chi,\ell,n}; \text{ire}_{r,\chi,\ell,n} < \text{ima}_{\chi,n} \}.$$

7. Image explicite des χ -lments cyclotomiques

la vue du corollaire 6.7 il est important de rendre explicite l'indice rsiduel

$$\text{ire}_{r,\chi,\ell,n} = \# \frac{\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1)\right)^\chi}{\phi_{\ell,n}^\chi(\langle c^F(r) \rangle^\chi)}.$$

Pour ce faire on donne d'abord une formule pour un $\mathbb{Z}_p[G]$ -gnrateur $c^F(r, \chi)$ de la χ -partie $\langle c^F(r) \rangle^\chi \subset \langle c^F(r) \rangle$ et pour un gnrateur de $\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1)\right)^\chi$, puis on donne une formule explicite pour $\phi_{\ell,n}(c^F(r, \chi))$. Par les propriets fonctorielles des χ -parties on a l'galit

$$\phi_{\ell,n}^\chi(\langle c^F(r) \rangle^\chi) = \langle \phi_{\ell,n}(c^F(r, \chi)) \rangle_{\mathbb{Z}_p[G]}.$$

L'indice rsiduel s'obtient alors en comparant $\phi_{\ell,n}(c^F(r, \chi))$ avec le gnrateur de $\left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times / p^n(r-1)\right)^\chi$.

Lemme 7.1. — *Soit G un groupe ablien et χ un caractre sur G . Soit*

$$S_\chi = \sum_{g \in \text{Ker } \chi} g \in \mathbb{Z}_p[G].$$

1. *Si p ne divise pas l'ordre $o(\chi)$ de χ , alors $\mathbb{Z}_p[G]^\chi \subset \mathbb{Z}_p[G]$ est l'idal principal engendr par*

$$T_\chi := S_\chi \frac{1}{o(\chi)} \sum_{g \in G/\text{Ker } \chi} \text{Tr}_{\mathbb{Z}_p[\chi]/\mathbb{Z}_p}(\chi(g))g^{-1}.$$

2. *Si p divise $o(\chi)$, soit $h \in G$ tel que $\chi(h) = \zeta_p$ et soit $\Delta \subset G/\text{Ker } \chi$ le sous-groupe des lments d'ordre premier p de $G/\text{Ker } \chi$. Alors $\mathbb{Z}_p[G]^\chi \subset \mathbb{Z}_p[G]$ est l'idal principal engendr par*

$$T_\chi := S_\chi(1-h) \frac{1}{o(\chi)} \sum_{\delta \in \Delta} \text{Tr}_{\mathbb{Z}_p[\chi(\Delta)]/\mathbb{Z}_p}(\chi(\delta))\delta^{-1}$$

3. *La χ -partie $(\mathbb{Z}/p^n[G])^\chi$ est le sous-module engendr par l'image mod p^n du gnrateur T_χ dfini en 1 ou 2 ci-dessous suivant que p divise ou pas $o(\chi)$.*

Démonstration. — On remarque pour commencer que les gnrateurs T_χ sont dfinis indpendamment des choix de $h \in G$ tel que $\chi(h) = \zeta_p$ et plus gnralement des choix des relvement des lments de $G/\text{Ker } \chi$ dans G grce au facteur S_χ qui neutralise ces choix. Soit $\tilde{\chi}$ le caractre sur $G/\text{Ker } \chi$ dduit de χ par factorisation. Il est bien connu que pour tout $\mathbb{Z}_p[G]$ -module M on a $M^\chi = (M^{\text{Ker } \chi})^{\tilde{\chi}}$. D'autre part $\mathbb{Z}_p[G]^{\text{Ker } \chi} = S_\chi \mathbb{Z}_p[G]$ et pour dmontrer 1 et 2 on peut donc supposer sans perte que χ est fidle sur G (cyclique). Maintenant pour voir 1 il suffit de reconnatre que l'lment $E_\chi = 1/o(G) \sum_{g \in G} \text{Tr}_{\mathbb{Z}_p[\chi]/\mathbb{Z}_p}(\chi(g))g^{-1}$ est l'idempotent \mathbb{Q}_p -rationnel usuel qui dfnit la fois la χ -partie et le χ -quotient de $\mathbb{Z}_p[G]$ pour tous les caractres conjugus de χ sur \mathbb{Q}_p . Le point 1 est dmontr.

Pour dmontrer 2 aussi on suppose χ fidle sur G cyclique. On peut crire $G = \Delta \times P$ o P est un p -groupe cyclique et dcomposer $\chi = \chi_1 \chi_2$ o χ_1 est la restriction de χ Δ et χ_2 la restriction de χ P . Pour tout $\mathbb{Z}_p[G]$ -module M on a les galits classiques $M^\chi = (M^{\chi_1})^{\chi_2} = (E_{\chi_1} M)^{\chi_2}$ et on se ramne donc dmontrer 2 dans le cas o $G = P$ est un p -groupe cyclique et χ est fidle sur G . Dans ce cas l'unique $h \in G$ tel que $\chi(h) = \zeta_p$ est un gnrateur de l'unique sous-groupe $C \subset G$ d'ordre p . Et par le lemme II.2 de [20] on a pour tout $\mathbb{Z}_p[G]$ -module M l'galit $M^\chi = \text{Ker } N_C$ o $N_C: M \rightarrow M$ est l'application norme suivant C dfinie par $N_C(m) = \sum_{g \in H} gm$. Dans le cas particulier o $M = \mathbb{Z}_p[G]$ alors M est C -cohomologiquement trivial et on a $\text{Ker } N_C = (1-h)\mathbb{Z}_p[G]$, ce qui conclut la preuve de 2.

Pour voir 3 on dfnit pour tout $\mathbb{Z}_p[G]$ -module M le module "tendu-tordu" $\mathcal{R}_{\chi, M}$ comme le $\mathbb{Z}_p[\chi]$ -module $\mathcal{R}_{\chi, M} = M \otimes \mathbb{Z}_p[\chi]$ muni de l'action de G tordue $g * x = \chi(g^{-1})gx$. Une minute de rflexion permet de s'assurer de l'isomorphie $M^\chi \cong \mathcal{R}_{\chi, M}^G$. Cela tant partant de la suite

$$0 \longrightarrow p^n \mathbb{Z}_p[G] \longrightarrow \mathbb{Z}_p[G] \longrightarrow \mathbb{Z}/p^n[G] \longrightarrow 0,$$

on obtient en passant aux χ -parties et en utilisant 1 ou 2 suivant que p divise ou pas $o(\chi)$ la suite :

$$0 \longrightarrow p^n T_\chi \mathbb{Z}_p[G] \longrightarrow T_\chi \mathbb{Z}_p[G] \longrightarrow (\mathbb{Z}/p^n[G])^\chi \longrightarrow H^1(G, \mathcal{R}_{\chi, p^n \mathbb{Z}_p[G]}).$$

Mais pour ce qui concerne le module libre $p^n \mathbb{Z}_p[G]$ son tendu-tordu $\mathcal{R}_{\chi, p^n \mathbb{Z}_p[G]}$ est encore isomorphe $\mathbb{Z}_p[\chi][G]$ qui est G -cohomologiquement trivial, d'o l'isomorphie requise $(T_\chi \mathbb{Z}_p[G])/p^n \cong (\mathbb{Z}/p^n[G])^\chi$. \square

Par le thorme 3.4 le module $\langle c^F(r) \rangle$ est $\mathbb{Z}_p[G]$ -libre et l'on dduit immdiatement du lemme 7.1 l'galit $\langle c^F(r) \rangle^\chi = \langle T_\chi c^F(r) \rangle$. D'o la proposition :

Proposition 7.2. — Soit χ un caractre sur G , soit $\Delta \subset G/\text{Ker } \chi$ le sous-groupe des lments d'ordre premier p de $G/\text{Ker } \chi$ et si $p \mid o(\chi)$ soit $h \in G$ tel que $\chi(h) = \zeta_p$. La χ -partie $\langle c^F(r) \rangle^\chi$ est le sous- $\mathbb{Z}_p[G]$ -module monogne engendr par

$$T_\chi c^F(r) = \begin{cases} \frac{1}{o(\chi)} \sum_{g \in G} \text{Tr}_{\mathbb{Z}_p[\chi]/\mathbb{Z}_p}(\chi(g^{-1})) g c^F(r) & \text{si } p \nmid o(\chi) \\ \frac{1-h}{o(\Delta)} \sum_{g \in G, p \nmid o(\chi(g))} \text{Tr}_{\mathbb{Z}_p[\chi]/\mathbb{Z}_p}(\chi(g^{-1})) g c^F(r) & \text{si } p \mid o(\chi) \end{cases}$$

Démonstration. — Les galits sont de simples r-critures de l'lment T_χ appliqu $c^F(r)$. \square

Proposition 7.3. — Soit $\ell \equiv 1[dp^n]$. On fixe $\xi_\ell \in \mathbb{Z}$ une racine primitive modulo ℓ telle que $\zeta_{dp^n} \equiv \xi_\ell^{(\ell-1)/dp^n} [\mathcal{L}(\lambda)]$, $o \lambda$ et $\mathcal{L}(\lambda)$ sont les idaux divisant ℓ fix pour la construction de $\phi_{\ell, n}$ en dbut de section 5. Partant de l'isomorphisme canonique $\text{Gal}(\mathbb{Q}(\zeta_{dp^n})/\mathbb{Q}) \cong (\mathbb{Z}/dp^n)^\times$, on fixe $I_{F, n}$ un systme de representants dans \mathbb{Z} de $\text{Gal}(\mathbb{Q}(\zeta_{dp^n})/F)$ et, pour tout $g \in G$, un representant $a_g \in \mathbb{Z}$ de g^{-1} . On a :

$$\phi_{\ell, n}(c^F(r)) = \left(\prod_{i \in I_{F, n}} (1 - \xi_\ell^{a_g i(\ell-1)/(dp^n)})^{i^{r-1}} \otimes t(r-1)_n \right)_{g \in G}.$$

Démonstration. — On a choisit ξ_ℓ pour avoir $\zeta_{dp^n} \equiv \xi_\ell^{(\ell-1)/dp^n} [\mathcal{L}(\lambda)]$, et donc aussi $\zeta_{dp^n}^{a_g} \equiv \xi_\ell^{a_g(\ell-1)/dp^n} [\mathcal{L}(\lambda)]$. Pour tout $g \in G$ soit $\sigma_g \in \text{Gal}(\mathbb{Q}(\zeta_{dp^n})/\mathbb{Q})$ le relvement de g tel que $\zeta_{dp^n} = \zeta_{dp^n}^{\sigma_g a_g}$ alors on a $\zeta_{dp^n} = \zeta_{dp^n}^{a_g \sigma_g} \equiv \xi_\ell^{a_g(\ell-1)/dp^n} [\mathcal{L}(\lambda)^\sigma]$, parce que σ agit

trivialement sur ξ_ℓ . On calcule maintenant $\phi_{\ell,n}(c^F(r))$:

$$\begin{aligned}
\phi_{\ell,n}(c^F(r)) &= \left(\text{res}_{\lambda^g}(\varphi_n(c^F(r))) \right)_{g \in G} \text{ par d'finition de } \phi_{\ell,n}, \\
&= \left(\text{red}_{\lambda^g}(r-1)(\varphi_n(c^F(r))) \right)_{g \in G} \text{ voir diagramme (12)} \\
&= \left(\text{red}_{\lambda^g}(r-1) \left(\sum_{\sigma} \kappa^{r-1}(\sigma) \sigma(1 - \zeta_{dp^n}) \otimes t(r-1)_n \right) \right)_{g \in G} \\
&\text{par la formule (7) et o } \sigma \text{ parcourt } \text{Gal}(\mathbb{Q}(\zeta_{dp^n})/F) \\
&= \left(\text{red}_{\lambda^g}(r-1) \left(\prod_{i \in I_{F,n}} (1 - \zeta_{dp^n}^i)^{i^{r-1}} \otimes t(r-1)_n \right) \right)_{g \in G} \\
&= \left(\prod_{i \in I_{F,n}} (1 - \xi_\ell^{a_g i(\ell-1)/(dp^n)})^{i^{r-1}} \otimes t(r-1)_n \right)_{g \in G}.
\end{aligned}$$

En effet la congruence $\zeta_{dp^n} \equiv \xi_\ell^{a_g(\ell-1)/dp^n} [\mathcal{L}(\lambda)^{\sigma_g}]$ dans $\mathbb{Q}(\zeta_{dp^n})$ remarque en dbut de preuve donne dans $F^\times/p^n(r-1)$:

$$\text{red}_{\lambda^g}(r-1) \left(\prod_{i \in I_{F,n}} (1 - \zeta_{dp^n}^i)^{i^{r-1}} \otimes t(r-1)_n \right) = \prod_{i \in I_{F,n}} (1 - \xi_\ell^{a_g i(\ell-1)/(dp^n)})^{i^{r-1}} \otimes t(r-1)_n.$$

Il faut aussi noter que la formule finale ne dpend plus des choix de a_g ou de σ_g puisque $\text{Gal}(\mathbb{Q}(\zeta_{dp^n})/F)$ agit trivialement de part et d'autre. \square

On a maintenant tous les lments pour donner une formule explicite calculant les quantits $\text{ire}_{r,\chi,\ell,n}$ qui interviennent dans le corollaire 6.7.

Thorme 7.4. — *Soit $\ell \equiv 1[dp]$ et soit $n \leq v_p(\ell-1)$. Pour tout groupe ablien M fini on note $M[p^n]$ les lments de M annuls par p^n . Soit η_ℓ une racine primitive modulo ℓ . On a*

$$(13) \quad \text{ire}_{r,\chi,\ell,n} = \# \frac{T_\chi \left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times[p^n] \right)}{\langle T_\chi \left(\prod_{i \in I_{F,n}} (1 - \eta_\ell^{a_g i(\ell-1)/(dp^n)})^{i^{r-1} \frac{\ell-1}{p^n}} \right)_{g \in G} \rangle_{\mathbb{Z}_p[\chi]}}$$

Démonstration. — L'indice

$$\# \frac{T_\chi \left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times/p^n(r-1) \right)}{\langle T_\chi \left(\prod_{i \in I_{F,n}} (1 - \xi_\ell^{a_g i(\ell-1)/(dp^n)})^{i^{r-1}} \otimes t(r-1)_n \right)_{g \in G} \rangle}$$

ne dpend pas du twist r choisi qu'on peut ainsi prendre $r = 1$ pour ce calcul. Ensuite si on prend $\eta_\ell = \xi_\ell$ on trouve d'aprs la proposition 7.3 et le lemme 7.1 l'galit

$$\text{ire}_{r,\chi,\ell,n} = \# \frac{T_\chi \left(\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times/p^n \right)}{\langle T_\chi \left(\prod_{i \in I_{F,n}} (1 - \eta_\ell^{a_g i(\ell-1)/(dp^n)})^{i^{r-1}} \right)_{g \in G} \rangle_{\mathbb{Z}_p[\chi]}}.$$

Clairement cette galit reste valable pour tout autre choix de racine primitive modulo ℓ que ξ_ℓ parce que l'indice de gauche dans l'galit (13) ne dpend pas de ce choix.

L'exponentiation par $(\ell - 1)/p^n$ réalise un isomorphisme entre $\mathbb{F}_\lambda^\times/p^n$ et $\mathbb{F}_\lambda^\times[p^n]$, ce qui conclut la preuve du thorme 7.4. \square

La formule finale (13) s'entend comme l'indice de deux $\mathbb{Z}_p[\chi]$ -modules monognes. Dans le cas particulier o l'ordre de χ divise $p-1$ alors $\mathbb{Z}_p[\chi]$ s'identifie \mathbb{Z}_p . Il est alors possible, comme c'est fait dans [15] p. 262, de dfinir des $c_{l,r,p^n}^\chi \in \mathbb{F}_l^\times$ et non dans un produit de $\mathbb{F}_\lambda^\times$; puis de calculer les $i_{r,\chi,l,n}$ comme des indices dans un seul \mathbb{F}_l^\times . Dans notre cadre plus gnral on peut avoir besoin de $[\mathbb{Q}_p(\chi) : \mathbb{Q}_p]$ paramtres p -adiques et on est contraint de travailler dans $\bigoplus_{g \in G} \mathbb{F}_{\lambda^g}^\times$. Cela augmente la complexit mais ne diminue pas l'effectivit de ces calculs d'indices.

Références

- [1] A. A. BEĬLISON – « Higher regulators of modular curves », Applications of algebraic K -theory to algebraic geometry and number theory, Part I, II (Boulder, Colo., 1983), Contemp. Math., vol. 55, Amer. Math. Soc., Providence, RI, 1986, p. 1–34.
- [2] T. BELIAEVA – « Unités semi-locales modulo sommes de Gauß en théorie d'Iwasawa », *Thèse de l'université de Franche-Comté Besançon* (2004).
- [3] J.-R. BELLIARD – « Global units modulo circular units : descent without Iwasawa's main conjecture », *Canad. J. Math.* **61** (2009), no. 3, p. 518–533.
- [4] D. BENOIS & T. NGUYËN-QUANG DÕ – « Les nombres de Tamagawa locaux et la conjecture de Bloch et Kato pour les motifs $\mathbb{Q}(m)$ sur un corps abélien », *Ann. Sci. École Norm. Sup. (4)* **35** (2002), no. 5, p. 641–672.
- [5] S. BLOCH & K. KATO – « L -functions and Tamagawa numbers of motives », The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, p. 333–400.
- [6] D. BURNS & C. GREITHER – « On the equivariant Tamagawa number conjecture for Tate motives », *Invent. Math.* **153** (2003), no. 2, p. 303–359.
- [7] R. F. COLEMAN – « Division values in local fields », *Invent. Math.* **53** (1979), no. 2, p. 91–116.
- [8] P. DELIGNE – « Le groupe fondamental de la droite projective moins trois points », Galois groups over \mathbf{Q} (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, p. 79–297.
- [9] W. GAJDA – « On cyclotomic numbers and the reduction map for the K -theory of the integers », *K-Theory* **23** (2001), no. 4, p. 323–343.
- [10] C. GREITHER – « Class groups of abelian fields, and the main conjecture », *Ann. Inst. Fourier (Grenoble)* **42** (1992), no. 3, p. 449–499.
- [11] A. HUBER & G. KINGS – « Bloch-Kato conjecture and Main Conjecture of Iwasawa theory for Dirichlet characters », *Duke Math. J.* **119** (2003), no. 3, p. 393–464.
- [12] A. HUBER & J. WILDESHAUS – « Classical motivic polylogarithm according to Beilinson and Deligne », *Doc. Math.* **3** (1998), p. 27–133 (electronic).
- [13] M. KOLSTER – « K -theory and arithmetic », Contemporary developments in algebraic K -theory, ICTP Lect. Notes, XV, Abdus Salam Int. Cent. Theoret. Phys., Trieste, 2004, p. 191–258 (electronic).
- [14] M. KOLSTER, T. NGUYËN QUANG DÕ & V. FLECKINGER – « Twisted S -units, p -adic class number formulas, and the Lichtenbaum conjectures », *Duke Math. J.* **84** (1996), no. 3, p. 679–717.
- [15] M. KURIHARA – « The Iwasawa λ -invariants of real abelian fields and the cyclotomic elements », *Tokyo J. Math.* **22** (1999), no. 2, p. 259–277.

- [16] J. NEUKIRCH, A. SCHMIDT & K. WINGBERG – *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000.
- [17] D. QUILLEN – « Higher algebraic K -theory. I », Algebraic K -theory, I : Higher K -theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972), Springer, Berlin, 1973, p. 85–147. Lecture Notes in Math., Vol. 341.
- [18] W. SINNOTT – « On the Stickelberger ideal and the circular units of a cyclotomic field », *Ann. of Math. (2)* **108** (1978), no. 1, p. 107–134.
- [19] ———, « On the Stickelberger ideal and the circular units of an abelian field », *Invent. Math.* **62** (1980), no. 2, p. 181–234.
- [20] D. SOLOMON – « On the classgroups of imaginary abelian fields », *Ann. Inst. Fourier (Grenoble)* **40** (1990), p. 467–492.
- [21] C. SOULÉ – « On higher p -adic regulators », Algebraic K -theory, Evanston 1980 (Proc. Conf., Northwestern Univ., Evanston, Ill., 1980), Springer, Berlin, 1981, p. 372–401.
- [22] ———, « Éléments cyclotomiques en K -théorie », *Astérisque* (1987), no. 147-148, p. 225–257, 344, Journées arithmétiques de Besançon (Besançon, 1985).
- [23] T. TSUJI – « Semi-local units modulo cyclotomic units », *J. Number Theory* **78** (1999), no. 1, p. 1–26.

4 décembre 2009

TATIANA BELIAEVA, IRMA, UMR 7501 de l'Université Louis Pasteur et du CNRS, 7 rue René Descartes, 67084 Strasbourg Cedex, France • *E-mail* : beliaeva@math.u-strasbg.fr
JEAN-ROBERT BELLIARD, Laboratoire de Mathématiques, UMR 6623 de l'Université de Franche-Comté et du CNRS, 16 route de Gray, 25030 Besançon cedex, France
E-mail : jean-robert.belliard@univ-fcomte.fr