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 $\left(H^1(G_S, \mathbb{Z}_p(r))^\chi : C^F(r)^\chi\right)$ 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 $\mathbb{F}_\ell$. 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 4
2. Éléments cyclotomiques et relations de normes tordues 6
3. Caractères des représentations en jeu 8
4. Composantes isotypiques 11
5. Les morphismes de réduction modulo ℓ 12
6. Le théorème d'indice 16
7. Image explicite des χ-éléments cyclotomiques 19
8. Quelques résultats numériques 22
Références 24

Introduction

Soit F un corps de nombres abélien totalement réel, d'anneau d'entiers O_F, de groupe de Galois $G = \mathrm{Gal}(F/\mathbb{Q})$ 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 $G_S = \mathrm{Gal}(\Omega_S/F)$. 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 $H^i(\mathrm{spec}\, O_F[1/p], \mathbb{Z}_p(r))$. Parmi les motivations à 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-adifiés $K_{2r-i}(O_F) \otimes \mathbb{Z}_p$ des groupes de K-théorie de Quillen (voir [**17**] pour la construction des groupes de K-théorie supérieurs). Cependant notre travail se situe entièrement en cohomologie galoisienne p-adique et est donc logiquement indépendant de ce contexte qui était conjectural au début de la rédaction de ce travail. Entre temps les travaux de Voevodsky, complétés par Weibel, ont aboutit à une démonstration de cette conjecture de Quillen-Lichtenbaum (voir [**24**]).

En arithmétique ces groupes de cohomologie p-adique s'interprètent comme des analogues supérieurs des groupes des p-unités (pour $i = 1$ et $r \notin \{0, 1\}$) et des p-groupes de S-classes d'idéaux (pour $i = 2$ et $r \geq 0$). Ces analogies sont précisées par une suite exacte due à Kolster, Nguyễn-Quang-Dỗ et Fleckinger pour $i = 1$ (voir theorem 3.2 de [**14**] p.689) et une suite exacte due à Kurihara pour $i = 2$ (voir lemma 4.3 de [**15**] p. 269). Ils sont aussi particulièrement intéressants à étudier en liaison avec les valeurs spéciales des fonctions L en $s = 1 - r$: ils sont au premier plan dans les démonstrations des conjectures à la Bloch-Kato pour les valeurs spéciales des fonctions L motiviques dans le cas particulier 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 pour F totalement réel abélien et $r > 1$ impair, conséquence du theorem 5.4 de [**14**] :

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

Ici $C^F(r)$ (voir la définition 2.4) est l'analogue supérieur des unités circulaires, et cette formule d'indice est donc l'analogue supérieur de la formule d'indice de Sinnott : une version algébrique de la formule analytique du nombre de classes de Dedekind. Cette formule d'indice passe aux χ-composantes lorsque $p \nmid [F : \mathbb{Q}]$, pour tout caractère χ sur $G = \mathrm{Gal}(F/\mathbb{Q})$ (c'est aussi une conséquence du theorem 5.4 de [**14**]). Lorsque $p \mid [F : \mathbb{Q}]$ l'indice $\left(H^1(G_S, \mathbb{Z}_p(r))^\chi : C^F(r)^\chi\right)$ et l'ordre $\#H^2(G_S, \mathbb{Z}_p(r))^\chi$ sont très probablement reliés, mais il y a a priori une déviation difficile à expliciter. Le principal résultat de cet article est de présenter une méthode explicite et élémentaire pour calculer les χ-indices $\left(H^1(G_S, \mathbb{Z}_p(r))^\chi : C^F(r)^\chi\right)$ pour tous les caractères de Dirichlet χ (voir le théorème 6.1, son corollaire 6.7 et la formulation explicite du théorème 7.4).

Dans l'article [**15**] Kurihara introduit une méthode remarquable pour calculer ces χ-indices en liaison avec l'ordre du $H^2(G_S, \mathbb{Z}_p(r))$, qu'il considère comme le p-adifié du groupe de Tate-Shafarevich associé au motif $h^0(\mathbb{Q}(\zeta_f))$. La méthode de Kurihara ramène le calcul de χ-indice à de l'arithmétique dans des corps finis $\mathbb{F}_\ell$, mais n'est complètement décrite dans l'article [**15**] que pour les caractères de Dirichlet χ dont l'ordre divise $p-1$. L'apport principal du présent article est de se dispenser de cette hypothèse restrictive. Pour ce faire on est parvenu à remplacer les considérations sur l'ordre de certains éléments spéciaux dans [**15**] par des isomorphismes canoniques et généraux de χ-composantes (voir le théorème 5.2).

Cet article est composé comme suit. Dans la section 1 on définit les notations $H^1(G_S, \mathbb{Z}_p(r))$ en justifiant les restrictions $r \geq 3$ impairs et F totalement réel. Puis

on rappelle la construction d'un morphisme de descente classique (voir par exemple [**14**]) $\overline{U}'_\infty(r-1)_{G_\infty} \xrightarrow{\alpha} H^1(G_S, \mathbb{Z}_p(r))$ où $\overline{U}'_\infty$ désigne la limite projective pour les normes des p-adifiés des p-unités des $F_n = F(\mu_{p^n})$ le long des étages finis de la tour $F_\infty = \bigcup_n F_n$ et où $G_\infty = \mathrm{Gal}(F_\infty/F)$. Il s'agit surtout, pour l'usage ultérieur fait dans cet article, de préciser explicitement les images de p-unités données.

Dans la section 2 on définit, en utilisant le morphisme α et suivant [**14**] et [**15**], les éléments cyclotomiques en cohomologie galoisienne $c_b^F(r)$ qui engendrent le groupe $C^F(r)$ et coïncident avec le p-adifiés des éléments cyclotomiques de Soulé ([**21**] ou aussi [**22**]) sous la conjecture de Quillen-Lichtenbaum. 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 $G = \mathrm{Gal}(F/\mathbb{Q})$-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 on utilise l'injectivité et la finitude du conoyau de α démontrées 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-clé (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 occasionnés 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 rappelées 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.

Dans la section 8 on donne quelques exemples numériques dans le cas ou F est un corps de degré p et χ est un caractère d'ordre p.

Remerciements : Les deux auteurs remercient Thong Nguyễn-Quang-Dõ qui nous a suggéré ce sujet comme une collaboration possible. La section 8 a été ajoutée à la demande du referee anonyme, nous le remercions aussi pour sa lecture attentive et

ses conseils constructifs. Ce travail doit énormément à Kurihara. D'abord l'article [**15**] nous a inspiré. Ensuite nous avons profité de ses conseils lors de la mise en forme finale. Nous lui en sommes particulièrement reconnaissant.

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 est un corps de nombres abélien totalement réel et $p \neq 2$ est 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 en dehors de S et $G_S = \mathrm{Gal}(\Omega_S/F)$ son groupe de Galois. On note aussi $\mathcal{G}_S = \mathrm{Gal}(\Omega_S/\mathbb{Q})$. Soit $F_n = F(\zeta_{p^n}) \subset \Omega_S$. On note $G_S(F_n)$ le groupe $\mathrm{Gal}(\Omega_S/F_n)$, on note $G_n = \mathrm{Gal}(F_n/F)$ et $G_\infty = \mathrm{Gal}(F_\infty/F) \cong \varprojlim G_n$, où $F_\infty = \bigcup_n F_n$.

La donnée du système compatible en norme ζ_{p^n} définit aussi un générateur $t(1)$ du module de Tate $\mathbb{Z}_p(1) := \varprojlim \mu_{p^n}$, où μ_m désigne le groupe des racines de l'unité 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 $r^{\text{ième}}$ de $t(1)$ qui est un générateur de $\mathbb{Z}_p(r) := \mathbb{Z}_p(1)^{\otimes r}$ et pour tout entier $n \geq 1$ on note $t(r)_n$ la $n^{\text{ième}}$ projection de $t(r)$ qui engendre $\mathbb{Z}/p^n(r)$. Si $\kappa\colon \mathcal{G}_S \twoheadrightarrow \mathbb{Z}_p^\times$ désigne le "caractère" cyclotomique, alors l'action de $\mathcal{G}_S$ sur $\mathbb{Z}_p(r)$ est donnée par $\gamma(x) = \kappa(\gamma)^r x$. Ces conventions permettent de définir pour tout entier $r \geq 1$ et tout $\mathbb{Z}_p[\mathcal{G}_S]$-module M son $r^{\text{ième}}$-tordu à la Tate, noté $M(r)$, 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-même muni de l'action de $\mathcal{G}_S$ tordue : $\gamma *_r x := \kappa(\gamma)^r \gamma(x)$. Le principal objet étudié 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, à un corps F totalement réel et supposer $r > 1$. Cette approche est basée sur l'existence d'éléments spéciaux 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 théorème 3.4). D'après les calculs de rang p. 223 de [**13**] la seule possibilité pour que $H^1(G_S, \mathbb{Z}_p(r))$ soit de $\mathbb{Z}_p$-rang égal à l'ordre de $G = \mathrm{Gal}(F/\mathbb{Q})$ est de prendre le corps F totalement réel 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-$p$-complétion du groupe des S-unités de F. Le twist $r = 1$ fait l'objet d'un nombre considérable de travaux, est connu pour être techniquement plus difficile et ne sera pas abordé dans cet article. L'un des avantages plus accessoires de ces restrictions en généralité est le lemme suivant :

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

Démonstration. — D'après le lemme 2.2 de [**14**] la torsion de $H^1(G_S, \mathbb{Z}_p(r))$ s'identifie à $\mathbb{Q}_p/\mathbb{Z}_p(r)^{G_\infty}$. Comme F est totalement réel la conjugaison complexe τ est un

élément bien défini de G_∞ qui vérifie $\kappa(\tau)^r = (-1)^r = -1$ puisque r est impair. Cet élément agit donc simultanément par multiplication par 1 et -1 sur $\mathbb{Q}_p/\mathbb{Z}_p(r)^{G_\infty}$ ce qui démontre que la torsion de $H^1(G_S, \mathbb{Z}_p(r))$ est annulé par 2. □

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

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

où $\overline{U}'_\infty$ désigne la limite projective relativement aux applications de norme des pro-p-complétions des S-unités $\overline{U}'_n = \overline{U}'_{F_n}$ le long de l'extension F_∞/F.

Soit $u_\infty = (u_n)_{n\in\mathbb{N}}$ une suite cohérente en norme de $\overline{U}'_\infty$ 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 $u_n \otimes t(r-1)_n$ définit un élément $x_n \in H^1(G_S(F_n), \mathbb{Z}/p^n(r))$. Concrètement 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

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

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

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

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 $\varphi_m\colon H^1(G_S, \mathbb{Z}_p(r)) \longrightarrow H^1(G_S(F_m), \mathbb{Z}/p^m(r))$ est la composée des applications (commutantes) de réduction modulo p^m et de restriction. On doit aussi remarquer que par définition $G_m = \mathrm{Gal}(F(\zeta_{p^m})/F)$ 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*

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

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

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 spéciaux

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

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 à ℓ par multiplication par ℓ est un élément bien défini de l'algèbre de groupe complète $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{bp^\infty}) \cap F_\infty/\mathbb{Q})]]$. Les éléments cyclotomiques sont liés par les relations de normes bien connues (pour tout premier ℓ et tout entier b avec $\ell b \mid d$) :

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

Le personnage principal de notre étude est le codescendu du r-ième tordu de ces éléments cyclotomiques.

Définition 2.1. — *On appelle r-ième élément spécial 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 $\varepsilon_{b,\infty}^F \otimes t(r-1) \in (\overline{U}'_\infty(r-1))_{G_\infty}$:*

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

L'élément spécial attaché à F sur lequel on s'attardera plus particulièrement est celui de conducteur d :

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

Ces éléments spéciaux sont caractérisés par leurs images contre les morphismes $\varphi_m \colon H^1(G_S, \mathbb{Z}_p(r)) \longrightarrow H^1(G_S(F_m), \mathbb{Z}/p^m(r))$.

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

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

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

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

Démonstration. — Pour obtenir (6) il suffit d'appliquer la formule (1) à la suite $(u_n) = \varepsilon_{b,\infty}$. Ici aussi les quantités $\kappa(g)$ sont bien définies modulo p^m parce que $\mathrm{Gal}(\mathbb{Q}(\zeta_{bp^m})/\mathbb{Q})$ opère sur μ_{p^m}. Pour en déduire la formule (7) on reprend la définition $\varepsilon_{b,m}^F = N_{\mathbb{Q}(\zeta_{bp^m})/F_m \cap \mathbb{Q}(\zeta_{bp^m})}(1 - \zeta_{bp^m})$. Or $\mathrm{Gal}(\mathbb{Q}(\zeta_{bp^m})/F_m \cap \mathbb{Q}(\zeta_{bp^m}))$ agit trivialement sur les racines p^m-ièmes de l'unités et donc pour $h \in \mathrm{Gal}(\mathbb{Q}(\zeta_{bp^m})/F_m \cap \mathbb{Q}(\zeta_{bp^m}))$ on

a $\kappa^{r-1}(h) \equiv 1[p^m]$. Par identification de G_m avec $\mathrm{Gal}(F_m \cap \mathbb{Q}(\zeta_{bp^m})/F \cap \mathbb{Q}(\zeta_{bp^m}))$ et par transitivité de la norme on obtient l'identité (7). □

Remarque : Par construction même, l'image dans $H^1(G_S(\mathbb{Q}(\zeta_f)), \mathbb{Z}_p(r))$ de l'élément spécial $c_b^F(r)$ est l'élément noté $c_r(\zeta_f)$ et appelé élément de Soulé-Deligne dans la définition 3.1.2 de [**11**]. Pour les liens entre ces éléments, ceux définis par Deligne dans [**8**], ceux définis par Soulé dans la section 4.4 de [**22**] (voir aussi [**21**]), ceux définis par Beilinson dans [**1**], voir les articles originaux et les comparaisons faites dans [**11**] et [**12**].

Proposition 2.3. — *Les r-ièmes éléments spéciaux de conducteurs différents sont liés par les relations de normes (pour tout nombre premier ℓ et tout b tel que $\ell b \mid d$) :*

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

Démonstration. — On remarque tout d'abord que $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell bp^\infty}) \cap F/\mathbb{Q}(\zeta_{bp^\infty}) \cap F)$ 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 à la Tate, donne :

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

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 :

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

Et on conclut à nouveau en prenant les co-invariants et en appliquant α. □

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-ièmes éléments spéciaux de conducteurs divisant d :*

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

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

Théorème 2.5. — *On rappelle que F est totalement réel et que $r > 1$ 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. — Soit G un groupe abélien agissant sur un corps de nombre K. Pour tout caractère χ sur G, si $p \nmid |G|$ on peut définir les χ-composantes avec des idempotents de $\mathbb{Z}_p[G]$. Toujours avec l'hypothèse $p \nmid |G|$, le passage à ces χ-composantes est exact. D'après [**14**] theorem 5.4, si K est une extension imaginaire,

absolument abélienne de F tel que $p \nmid [K : F]$ on a pour tout χ sur G tel que $\chi(-1) = (-1)^{r-1}$:

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

(Noter la différence de notation entre [**14**] et le présent article, les rôles de K et F sont inversés et la notation $\overline{C}'(r-1)_{G_\infty}$ est ici allégée en $C^K(r)$.) Maintenant pour démontrer la formule du théorème 2.5 il suffit de prendre $K = F[i]$ et comme $p \neq 2$ le théorème s'applique avec χ le caractère trivial sur $\mathrm{Gal}(K/F)$ et $r > 1$ impair. □

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 étant précisée notamment par la suite exacte (2) ; tandis que les $H^2(G_S, \mathbb{Z}_p(r))$ se comportent comme des p-groupes de S-classes d'idéaux 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**]).

Remarque : Lorsque $p \nmid [F : \mathbb{Q}]$ la démarche de [**14**] s'applique aussi pour démontrer la formule

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

pour tout caractère χ sur F. Le referee demande que soit précisé l'état des connaissances sur l'égalité entre les ordres des χ-parties (respectivement des χ-quotients) des modules ci-dessus lorsque p divise le degré $[F : \mathbb{Q}]$. C'est une question difficile, dont la réponse dépend a priori du choix entre χ-parties et χ-quotient, et n'est pas connue des auteurs.

Il est de toute façon 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, traité 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 auxquelles on s'intéresse, on calcule le caractère de quelques représentations linéaires.

3. Caractères des représentations en jeu

Définition 3.1. — *Soit G un groupe fini.*

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

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

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

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 caractère commun sur $\mathrm{Gal}(F/\mathbb{Q})$ 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 caractère régulier.*

Démonstration. — 1– est une conséquence du théorème 5.4 de [**14**] et 2– de la suite exacte (2). Pour 3– il suffit de calculer le caractère de $(\overline{U}'_\infty(r-1))_{G_\infty}$ par injectivité de α. Parce que r est impair et F totalement réel, ce caractère est le caractère régulier, autrement dit $(\overline{U}'_\infty(r-1))_{G_\infty} \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[G]$. Ce résultat fait probablement partie du folklore et par exemple est compatible avec les rangs mentionnés dans [**13**]. Nous n'avons malheureusement pas trouvé de référence qui précise le caractère des modules qui interviennent dans cet article. Pour la commodité du lecteur on va énoncer et refaire la preuve du lemme à suivre qui conclut la démonstration de la proposition 3.2. □

Lemme 3.3. — *Soit $\mathcal{U}_\infty$ (resp. $\overline{U}_\infty$) la limite projective des unités 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 caractère de $\mathcal{U}_\infty(r)_{G_\infty}$ est le caractère régulier. Le caractère de $\mathcal{U}_\infty(-1)_{G_\infty}$ est la somme du caractère régulier et de celui de $\mathbb{Z}_p[S]$.*
2. *Si r est pair alors le module $\overline{U}_\infty(r)_{G_\infty}$ est de caractère régulier. Le caractère de $\overline{U}_\infty(-1)_{G_\infty}$ est le caractère de $\mathbb{Z}_p$ avec action triviale de G. Si r est impair et différent de -1 alors $\overline{U}_\infty(r)_{G_\infty}$ est de $\mathbb{Z}_p$-torsion.*
3. *Les modules $\overline{U}_\infty(r)_{G_\infty}$ et $\overline{U}'_\infty(r)_{G_\infty}$ ont même caractère.*

Démonstration. — On note $\mathcal{G} = \mathrm{Gal}(F_\infty/\mathbb{Q})$ et $\Lambda[\mathcal{G}]$ l'algèbre de groupe pro-p-complété de $\mathcal{G}$. Clairement on a $\Lambda[\mathcal{G}] \cong \Lambda[\mathcal{G}](r)$ pour tout r. Lorsque p est modérément ramifié dans F, la théorie de Coleman donne une suite exacte (voir [**10**] ou [**23**] pour les détails)

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

Sans aucune condition de ramification mais si F est abélien sur $\mathbb{Q}$ il existe un sous-corps $L \subset F_\infty$ qui est abélien sur $\mathbb{Q}$, dans lequel p est modérément ramifié, 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 abélien.

On vérifie 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'égalité $\mathcal{V}_\infty(-1)^{G_\infty} = 0$ 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 caractères sont additifs en suites exactes cela démontre 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 caractère est nul. La même chasse au diagramme que ci-dessus mais en plus simple démontre donc que $\mathcal{U}_\infty(r)_{G_\infty}$ et $\Lambda[\mathcal{G}]_{G_\infty}$ ont même caractère, c'est-à-dire le caractère régulier. Le point 1 est démontré.

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 déduit $\mathcal{U}_\infty(r)_{G_\infty} = (\mathcal{U}^+_\infty\oplus\mathcal{U}^-_\infty)(r)_{G_\infty} = \mathcal{U}^+_\infty(r)_{G_\infty}$. Par la conjecture faible de Leopoldt, qui est un théorème pour l'extension cyclotomique, on sait que $\mathcal{U}^+_\infty/\overline{U}^+_\infty$ est un module de torsion de type fini sur l'algèbre d'Iwasawa classique $\Lambda = \Lambda[\mathrm{Gal}(F_\infty/F(\zeta_p))]$. 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 conséquence les modules $(\mathcal{U}^+_\infty/\overline{U}^+_\infty)(r)^{G_\infty}$ et $(\mathcal{U}^+_\infty/\overline{U}^+_\infty)(r)_{G_\infty}$ ont même caractère. Dans cette parité de r le point 2 se déduit donc du point 1 et de la suite exacte

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

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

On démontre le point 3. Les modules $\overline{U}_\infty$ et $\overline{U}'_\infty$ ont la même Λ-torsion (à savoir $\mathbb{Z}_p(1)$) et donc $\overline{U}'_\infty(r)$ et $\overline{U}_\infty(r)$ ont les même G_∞ invariants (à 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 démontre le point 3 en suivant le même type de chasse au diagramme que précédemment.

□

On énonce un premier résultat utile à notre calcul de χ-indice :

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

Démonstration. — Comme on étudie le module monogène engendré par $c^F(r)$, il suffit de montrer que pour tout caractère de Dirichlet χ sur G l'élément $c^F(r)\otimes e_\chi \in C^F(r)\otimes\mathbb{C}_p$ est non nul, où e_χ désigne l'idempotent usuel $e_\chi = (1/\#G)\sum_g \chi(g)g^{-1}$. On fixe χ un tel caractère, on note F_χ le sous-corps de F fixé par $\mathrm{Ker}\,\chi$ et on note kp^s le conducteur commun à χ et à 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 engendré par les $c^F_b(r)\otimes e_\chi$. 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 $c^F_b(r)\otimes e_\chi$ est nul parce que tout élément non trivial g de $\mathrm{Gal}(F_\chi/\mathbb{Q}(\zeta_{bp^\infty})\cap F_\chi)$ agit simultanément par multiplication par 1 et par $\chi(g) \neq 1$ sur $c^F_b(r)\otimes e_\chi$. Par contre tous les $c^F_b(r)\otimes e_\chi$ pour tous les b tels que $\mathbb{Q}(\zeta_{bp^\infty})$ contienne F_χ sont co-linéaires à $c^F_k(r)\otimes e_\chi$. En effet la formule (8) donne :

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

c'est-à-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 eulériens $(1-\ell^{r-1}\chi(\ell)^{-1})$ 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 définitions des χ-parties et χ-quotients et l'on décrit précisément quel χ-indice est calculé dans la suite en expliquant nos choix.

Définition 4.1. — *Soit M un $\mathbb{Z}_p[G]$-module et χ un caractère 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 décrite par χ. Formellement on peut définir M^χ par*
$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(\underline{\mathbb{Z}_p[\chi]},M)\cong M^\chi\subset M.$$
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 décrite par χ. Formellement on peut définir M_χ par*
$$M\twoheadrightarrow M_\chi\cong M\otimes_{\mathbb{Z}_p[G]}\underline{\mathbb{Z}_p[\chi]}.$$

Pour les propriétés basiques de ces deux foncteurs on pourra consulter le §II de [**20**], la section 2 de [**23**], ou la thèse du premier auteur [**2**]. Il serait beau d'avoir des méthodes 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 général ne coïncident pas forcément. Dans la suite on choisit de calculer $\#(H^1(G_S,\mathbb{Z}_p(r))^\chi/\langle c^F(r)\rangle^\chi)$, qui se prête le mieux à l'approche de cet article, par exemple en raison du théorème 3.4. Très souvent (en particulier par exemple si $p\nmid[F:\mathbb{Q}]$) tous ces χ-indices sont égaux. Mais dans la généralité avec laquelle cet article est rédigé il semble utile d'expliquer ce choix. Dans le but d'étudier l'arithmétique des valeurs spéciales d'une fonction L de Dirichlet (primitive) $L(s,\chi)$ il est naturel de fixer un caractère de Dirichlet χ de conducteur f, de prendre $F=F_\chi:=\mathbb{Q}(\zeta_f)^{\mathrm{Ker}\,\chi}$ et d'utiliser le module monogène engendré par l'élément cyclotomique $\langle c^F(r)\rangle$ à la place du module $C^F(r)$. Dans cette restriction (naturelle) en généralité, on a alors G cyclique, et notre choix n'est pas restrictif à cause de la proposition suivante :

Proposition 4.2. — *On suppose G cyclique.*

1. *Pour tout $\mathbb{Z}_p[G]$-module fini M on a $\#M^\chi=\#M_\chi$, en particulier on a l'égalité*
$$\#\left(\frac{H^1(G_S,\mathbb{Z}_p(r))}{\langle c^F(r)\rangle}\right)^\chi=\#\left(\frac{H^1(G_S,\mathbb{Z}_p(r))}{\langle c^F(r)\rangle}\right)_\chi.$$

2. *On a un isomorphisme*

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

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

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

Cela donne l'égalité des ordres du point 1.

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

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

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

Comme cela ne présente pas de difficultés supplémentaires, dans la suite on prend F abélien totalement réel quelconque, on prend χ un caractère sur G quelconque et l'on va calculer l'indice $\#(H^1(G_S,\mathbb{Z}_p(r))^\chi/\langle c^F(r)\rangle^\chi)$ en utilisant les morphismes de réduction modulo ℓ dans le style de Kurihara [**15**].

5. Les morphismes de réduction modulo ℓ

Soit un entier $n \geq 1$ et étant donné un nombre premier $\ell \in \mathbb{Z}$, tel que $\ell \equiv 1[dp^n]$, et un idéal fixé λ de F divisant ℓ, l'objet de cette section est de construire explicitement et de décrire des propriétés d'une application de réduction G-équivariante :

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

où $\mathbb{F}_\lambda$ désigne le corps résiduel $O_F/\lambda \cong \mathbb{F}_\ell$. Cette application $\phi_{\ell,n}$ est essentiellement "l'application naturelle" de [**15**] p. 265, mais pour l'usage ultérieur fait dans cet article on l'examine un peu plus en détail ici. Dans l'article [**9**] Gajda examine aussi une application naturelle en K-théorie $\phi_{p,l}\colon K_{2n+1}(\mathbb{Z}) \longrightarrow K_{2n+1}(\mathbb{F}_p)[l^\infty]$. Sous la conjecture de Quillen-Lichtenbaum, via les classes de Chern, le $\phi_{l,p}$ de Gajda donne ainsi une application naturelle de réduction pour le cas particulier où le corps F est un sous-corps de $\mathbb{Q}(\zeta_p)$. En supposant l'hypothèse de Vandiver, Gajda démontre que son $\phi_{l,p}$ est non nul pour un ensemble de premiers p dont il calcule la densité. Notre démarche requiert des informations plus précises que la non trivialité des $\phi_{\ell,n}$ et se situe en cohomologie Galoisienne.

On rappelle que $\mathcal{G}_S$ désigne $\mathrm{Gal}(\Omega_S/\mathbb{Q})$. Pour tout idéal premier λ de O_F divisant $\ell \equiv 1[dp]$, on se donne un idéal $\mathcal{L} = \mathcal{L}(\lambda)$ de Ω_S divisant λ. Soit $D_\mathcal{L} \subset G_S$ le sous-groupe de décomposition 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 $res_\lambda\colon H^1(G_S,M) \longrightarrow$

$H^1(D_{\mathcal{L}}, M)$. Si on se donne en outre $\sigma \in \mathcal{G}_S$, alors cette restriction commute avec le morphisme de conjugaison σ_* qui définit l'action de σ sur les $H^1(H, M)$ pour tout sous-groupe fermé H de $\mathcal{G}_S$ (voir par exemple [**16**] p. 44). Ainsi modulo l'identification $D_{\mathcal{L}} \overset{\sigma}{\cong} D_{\mathcal{L}^\sigma}$ ce morphisme de restriction dépend 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 définit un idéal λ^σ de F divisant ℓ on a un diagramme commutatif

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

Si $\lambda \notin S$, alors λ est non ramifié dans Ω_S et le pro-p-quotient maximal de $D_{\mathcal{L}}$ s'identifie avec le pro-p-quotient maximal de $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\lambda)$. 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 posé on construit un morphisme $\phi_{\ell,n}$ comme annoncé dans le diagramme (10) en prenant $M = \mathbb{Z}/p^n(r)$ dans ce qui précède et en posant

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

On obtient alors immédiatement que $\phi_{\ell,n}$ est G-équivariant 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 interprétation kummerienne.

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

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

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

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

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

Cette définition permet de calculer explicitement les images de res_λ en utilisant le diagramme commutatif suivant :

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

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

Le résultat principal de cette section est le théorème d'isomorphisme suivant qui permet d'utiliser les morphismes de réduction pour calculer les χ-indices :

Théorème 5.2. — *Soit χ un caractère de $\mathrm{Gal}(F/\mathbb{Q})$. On Rappelle que f, le conducteur de F, vaut $f = dp^a$ avec $p \nmid d$. On prend un $n > a$. Il existe un (une infinité 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 :*

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

Démonstration. — Tout d'abord les deux modules sont finis, isomorphes sur $\mathbb{Z}_p[G]$ à $\mathbb{Z}_p[\chi]/p^n$. 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 caractère régulier (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 évident. Il suffit donc de trouver un (une infinité de) ℓ tels que l'application

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

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

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

L'injectivité 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'injectivité du morphisme (2) suit par la suite d'inflation restriction grâce à la $\mathrm{Gal}(F_n/F)$-trivialité cohomologique des $\mathbb{Z}/p^n(r)$ pour $r \neq 0$ (lemme de Tate). L'injectivité du morphisme (3) vient de la théorie de Kummer et a déjà été affirmée 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 théorème de Dirichlet $\mathbb{L}_n$ est infini. On considère l'application de réduction $red(r-1)$ produit des $red_\lambda(r-1)$ pour λ parcourant les premiers de F divisant les $\ell \in \mathbb{L}_n$:

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

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 vérifier cette injectivité pour $r=1$. Soit $\varphi\colon F_n^\times \longrightarrow \prod_{\ell\in\mathbb{L}_n}\left(\prod_{\lambda|\ell,\lambda\subset F}\mathbb{F}_\lambda^\times\right)$ l'application de réduction avant de prendre le quotient modulo p^n. Si x est dans le noyau de φ alors $(x-1)$ appartient à tous les $\mathcal{L}$ avec $v_\mathcal{L}(x)=0$ soit une infinité d'idéaux premiers distincts, et donc $x=1$. Cela montre l'injectivité de φ. On en déduit un morphisme injectif

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

L'image de $\imath$ est contenu dans les éléments d'ordre une puissance de p du quotient de droite. Ce sous-groupe des éléments d'ordre une puissance de p s'injecte lui-même 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 $\ell\in\mathbb{L}_n$. □

On reprend la preuve du théorème 5.2. Par exactitude à gauche du foncteur χ-parties on déduit de ce qui précède une suite de morphismes injectifs :

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

Pour un ℓ fixé, l'application déduite par χ-partie de $\phi_{\ell,n}$ est la composée 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 conséquence de la commutativité du diagramme (12) (compatibilité entre res_λ et $red_\lambda(r-1)$). On fixe x un $\mathbb{Z}_p[\chi]$-générateur 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 forcément de même pour au moins une des projections $\phi^\chi_{\ell,n}(x)$ et donc pour au moins un $\ell\in\mathbb{L}_n$. En outre le même raisonnement s'applique si on remplace $\mathbb{L}_n$ par n'importe lequel de ses sous-ensemble infini $\mathcal{E}\subset\mathbb{L}_n$. Donc il existe aussi une infinité de $\ell\in\mathbb{L}_n$ tel que $\phi^\chi_{\ell,n}$ soit un isomorphisme : cela démontre le théorème 5.2. □

6. Le théorème d'indice

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

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

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

Théorème 6.1. —

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

Dans la section 7 on décrira concrètement le module $\phi^{\chi}_{\ell,n}(\langle c^F(r) \rangle^{\chi})$, ce qui permettra de reformuler le théorème 6.1 de façon plus explicite.

Remarque : Un énoncé analogue au théorème 6.1 avec des χ-quotients à la place de χ-parties est certainement vrai. Néanmoins, l'approche présente, qui s'appuie sur des morphismes injectifs, ne s'applique pas ; et c'est l'une des raisons de choisir les χ-parties pour cet article. Pour calculer les ordres χ-quotients en jeu ici il faudrait développer une méthode de démonstration complètement différente.

La suite de cette section est consacrée à la démonstration de ce théorème 6.1, qui passe par quelques énoncés intermédiaires intéressants en eux-mêmes. On commence par introduire des abréviations commodes.

Définition 6.2. — *On rappelle que F est abélien totalement réel de conducteur $p^a d$ avec $p \nmid d$.*

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

Avec ces notations on a la relation d'indice :

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

$$\# \frac{H^{\chi}_{S,r}/p^n H^{\chi}_{S,r}}{C^{\chi}_{F,r}/(C^{\chi}_{F,r} \cap p^n H^{\chi}_{S,r})} \;\leq\; \# \frac{\left(\bigoplus_{g \in G} \mathbb{F}^{\times}_{\lambda^g}/p^n(r-1) \right)^{\chi}}{\phi^{\chi}_{\ell,n}(C^{\chi}_{F,r}/(C^{\chi}_{F,r} \cap p^n H^{\chi}_{S,r}))}.$$

Démonstration. — On avait déjà fait remarquer que les modules finis $H^{\chi}_{S,r}/p^n$ et $(\bigoplus_{g \in G} \mathbb{F}^{\times}_{\lambda^g}/p^n(r-1))^{\chi}$ sont tous deux isomorphes à $\mathbb{Z}_p[\chi]/p^n$ donc en particulier ils ont même ordre. Le lemme se ramène donc à l'inégalité évidente

$$\# \phi^{\chi}_{\ell,n}(C^{\chi}_{F,r}/(C^{\chi}_{F,r} \cap p^n H^{\chi}_{S,r})) \leq \# C^{\chi}_{F,r}/(C^{\chi}_{F,r} \cap p^n H^{\chi}_{S,r}).$$

□

L'inégalité du lemme 6.3 conduit à l'égalité avec le $\min_{\ell\in\mathbb{L}'_n}$ du théorème 6.1. Il suffit juste d'observer que ce min est actuellement atteint. C'est l'objet du second lemme intermédiaire qui est une conséquence immédiate du théorème 5.2 :

Lemme 6.4. — *Soit $n\in\mathbb{N}$.*

1. *Si $\ell\in\mathbb{L}_n^{\mathrm{iso}}$ alors l'isomorphisme $\phi_{\ell,n}^{\chi}$ induit un isomorphisme :*
$$\frac{H_{S,r}^{\chi}/p^nH_{S,r}^{\chi}}{C_{F,r}^{\chi}/(C_{F,r}^{\chi}\cap p^nH_{S,r}^{\chi})}\ \xrightarrow{\sim}\ \frac{\left(\bigoplus_{g\in G}\mathbb{F}_{\lambda^g}^{\times}/p^n(r-1)\right)^{\chi}}{\phi_{\ell,n}^{\chi}(C_{F,r}^{\chi}/(C_{F,r}^{\chi}\cap p^nH_{S,r}^{\chi}))}.$$
2. *Pour tout $\ell\in\mathbb{L}_n^{\mathrm{iso}}$ l'inégalité d'ordre du lemme 6.3 est une égalité.*
3. *Si en outre n est tel que $p^nH_{S,r}^{\chi}\subset C_{F,r}^{\chi}$ et $\ell\in\mathbb{L}_n^{\mathrm{iso}}$ alors $\phi_{\ell,n}^{\chi}$ induit un isomorphisme :*
$$\frac{H_{S,r}^{\chi}}{C_{F,r}^{\chi}}\ \xrightarrow{\sim}\ \frac{\left(\bigoplus_{g\in G}\mathbb{F}_{\lambda^g}^{\times}/p^n(r-1)\right)^{\chi}}{\phi_{\ell,n}^{\chi}(C_{F,r}^{\chi})}.$$

Démonstration. — Par définition même de $\mathbb{L}_n^{\mathrm{iso}}$ si $\ell\in\mathbb{L}_n^{\mathrm{iso}}$ alors l'homomorphisme
$$\phi_{\ell,n}^{\chi}\colon H_{S,r}^{\chi}/p^n\longrightarrow\left(\bigoplus_{g\in G}\mathbb{F}_{\lambda^g}^{\times}/p^n(r-1)\right)^{\chi}$$
est un isomorphisme. On déduit l'isomorphisme du point 1 en passant au quotient à gauche par $C_{F,r}^{\chi}/(C_{F,r}^{\chi}\cap H_{S,r}^{\chi})$ et à droite par son image. Le point 2 est une conséquence directe du point 1. Pour démontrer le point 3, à partir des égalités $C_{F,r}^{\chi}\cap p^nH_{S,r}^{\chi}=p^nH_{S,r}^{\chi}$ et $C_{F,r}^{\chi}+p^nH_{S,r}^{\chi}=C_{F,r}^{\chi}$, il suffit d'observer les isomorphismes évidents :
$$\frac{H_{S,r}^{\chi}}{C_{F,r}^{\chi}}\cong\frac{H_{S,r}^{\chi}}{C_{F,r}^{\chi}+p^nH_{S,r}^{\chi}}\cong\frac{H_{S,r}^{\chi}/p^nH_{S,r}^{\chi}}{C_{F,r}^{\chi}/p^nH_{S,r}^{\chi}}\cong\frac{H_{S,r}^{\chi}/p^nH_{S,r}^{\chi}}{C_{F,r}^{\chi}/(C_{F,r}^{\chi}\cap p^nH_{S,r}^{\chi})}.$$
□

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

Théorème 6.5. — *Pour tout $n\in\mathbb{N}$ on a l'égalité*
$$\#\frac{H_{S,r}^{\chi}/p^nH_{S,r}^{\chi}}{C_{F,r}^{\chi}/(C_{F,r}^{\chi}\cap p^nH_{S,r}^{\chi})}\ =\ \min_{\ell\in\mathbb{L}'_n}\left(\#\frac{\left(\bigoplus_{g\in G}\mathbb{F}_{\lambda^g}^{\times}/p^n(r-1)\right)^{\chi}}{\phi_{\ell,n}^{\chi}(\langle c^F(r)\rangle^{\chi})}\right)$$

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

On démontre maintenant le théorème 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 $C_{F,r}^{\chi}\subset p^nH_{S,r}^{\chi}$, ce qui a lieu pour $n=0$ et devient faux dès que n est suffisamment grand.

– soit $p^n H^\chi_{S,r} \subset C^\chi_{F,r}$, ce qui a lieu dès que $n \geq N$ pour un certain N.
Cela étant, tant que $n < N$ l'approximation modulo p^n ne donne aucune information puisque :

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

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

$$\frac{H^\chi_{S,r}/p^n H^\chi_{S,r}}{C^\chi_{F,r}/(C^\chi_{F,r} \cap p^n H^\chi_{S,r})} \cong \frac{H^\chi_{S,r}/p^n H^\chi_{S,r}}{C^\chi_{F,r}/p^n H^\chi_{S,r}} \cong \frac{H^\chi_{S,r}}{C^\chi_{F,r}}$$

De plus dès que $n > N$ on aura

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

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

Une autre façon, peut-être plus propice aux approches numériques, de formuler le théorème 6.1 consiste à 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 résiduel $\#\dfrac{\left(\bigoplus_{g\in G} \mathbb{F}^\times_{\lambda^g}/p^n(r-1)\right)^\chi}{\phi^\chi_{\ell,n}(\langle c^F(r)\rangle^\chi)}$, soit strictement inférieur à l'indice maximal $\#\mathbb{Z}_p[\chi]/p^n$. C'est une façon de comprendre l'introduction d'indices étoilés par exemple p.261 de [**15**]. De ce point de vue, on peut éviter le $\max_n$ du théorème 6.1. Pour cela on définit d'abord des notations supplémentaires :

Définition 6.6. — *On rappelle que $\mathbb{L}'_1$ désigne 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* $\mathrm{ire}_{r,\chi,\ell,n}$ *(pour indice résiduel) la quantité :*

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

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

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

Avec ces notations, pour remplacer le maximin du théorème 6.1 par un simple min, il suffit d'écarter les cas d'égalité entre indice résiduel et indice maximal. Cela conduit au corollaire :

Corollaire 6.7. —

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

7. Image explicite des χ-éléments cyclotomiques

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

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

Pour ce faire on donne d'abord une formule pour un $\mathbb{Z}_p[G]$-générateur $c^F(r,\chi)$ de la χ-partie $\langle c^F(r)\rangle^{\chi} \subset \langle c^F(r)\rangle$ et pour un générateur 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 propriétés fonctorielles des χ-parties on a l'égalité

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

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

Lemme 7.1. — *Soit G un groupe abélien et χ un caractère sur G. Soit*

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

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'idéal principal engendré par*

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

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

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

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

Démonstration. — On remarque pour commencer que les générateurs T_χ sont définis indépendamment des choix de $h \in G$ tel que $\chi(h) = \zeta_p$ et plus généralement des choix des relèvement des éléments de $G/\,\mathrm{Ker}\,\chi$ dans G grâce au facteur S_χ qui neutralise ces choix. Soit $\widetilde{\chi}$ le caractère sur $G/\,\mathrm{Ker}\,\chi$ déduit de χ par factorisation. Il est bien connu que pour tout $\mathbb{Z}_p[G]$-module M on a $M^{\chi} = (M^{\mathrm{Ker}\,\chi})^{\widetilde{\chi}}$. D'autre part $\mathbb{Z}_p[G]^{\mathrm{Ker}\,\chi} = S_\chi\mathbb{Z}_p[G]$ et pour démontrer 1 et 2 on peut donc supposer sans perte que χ est fidèle sur G (cyclique). Maintenant pour voir 1 il suffit de reconnaître que l'élément $E_\chi = 1/o(G)\sum_{g\in G} Tr_{\mathbb{Z}_p[\chi]/\mathbb{Z}_p}(\chi(g))g^{-1}$ est l'idempotent $\mathbb{Q}_p$-rationnel usuel qui définit à la fois la χ-partie et le χ-quotient de $\mathbb{Z}_p[G]$ pour tous les caractères conjugués de χ sur $\mathbb{Q}_p$. Le point 1 est démontré.

Pour démontrer 2 aussi on suppose χ fidèle sur G cyclique. On peut écrire $G = \Delta\times P$ où P est un p-groupe cyclique et décomposer $\chi = \chi_1\chi_2$ où χ_1 est la restriction de χ à Δ et χ_2 la restriction de χ à P. Pour tout $\mathbb{Z}_p[G]$-module M on a les égalités

classiques $M^\chi = (M^{\chi_1})^{\chi_2} = (E_{\chi_1} M)^{\chi_2}$ et on se ramène donc à démontrer 2 dans le cas où $G = P$ est un p-groupe cyclique et χ est fidèle sur G. Dans ce cas l'unique $h \in G$ tel que $\chi(h) = \zeta_p$ est un générateur 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'égalité $M^\chi = \operatorname{Ker} N_C$ où $N_C \colon M \longrightarrow M$ est l'application norme suivant C définie par $N_C(m) = \sum_{g \in H} gm$. Dans le cas particulier où $M = \mathbb{Z}_p[G]$ alors M est C-cohomologiquement trivial et on a $\operatorname{Ker} N_C = (1-h)\mathbb{Z}_p[G]$, ce qui conclut la preuve de 2.

Pour voir 3 on définit pour tout $\mathbb{Z}_p[G]$-module M le module "étendu-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 réflexion permet de s'assurer de l'isomorphie $M^\chi \cong (\mathcal{R}_{\chi,M})^G$. Ceci posé, en 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 étendu-tordu $\mathcal{R}_{\chi,p^n\mathbb{Z}_p[G]}$ est encore isomorphe à $\mathbb{Z}_p[\chi][G]$ qui est G-cohomologiquement trivial, d'où l'isomorphie requise $(T_\chi\mathbb{Z}_p[G])/p^n \cong (\mathbb{Z}/p^n[G])^\chi$. $\square$

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

Proposition 7.2. — *Soit χ un caractère sur G, soit $\Delta \subset G/\operatorname{Ker}\chi$ le sous-groupe des éléments d'ordre premier à p de $G/\operatorname{Ker}\chi$ 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 monogène engendré par*

$$T_\chi c^F(r) = \begin{cases} \dfrac{1}{o(\chi)} \displaystyle\sum_{g \in G} Tr_{\mathbb{Z}_p[\chi]/\mathbb{Z}_p}(\chi(g^{-1}))gc^F(r) \ \textit{si } p \nmid o(\chi) \\ \dfrac{1-h}{o(\Delta)} \displaystyle\sum_{g \in G, p \nmid o(\chi(g))} Tr_{\mathbb{Z}_p[\chi]/\mathbb{Z}_p}(\chi(g^{-1}))gc^F(r) \ \textit{si } p \mid o(\chi) \end{cases}$$

Démonstration. — Les égalités sont de simples ré-écritures de l'élément T_χ appliqué à $c^F(r)$. $\square$

Proposition 7.3. — *Soit $\ell \equiv 1[dp^n]$. On fixe $\xi_\ell \in \mathbb{Z}$ une racine primitive modulo ℓ telle que $\zeta_{dp^n} \equiv \xi_\ell^{(\ell-1)/dp^n}[\mathcal{L}(\lambda)]$, où λ et $\mathcal{L}(\lambda)$ sont les idéaux divisant ℓ fixé pour la construction de $\phi_{\ell,n}$ en début de section 5. Partant de l'isomorphisme canonique $\operatorname{Gal}(\mathbb{Q}(\zeta_{dp^n})/\mathbb{Q}) \cong (\mathbb{Z}/dp^n)^\times$, on fixe $I_{F,n}$ un système de représentants dans $\mathbb{Z}$ de $\operatorname{Gal}(\mathbb{Q}(\zeta_{dp^n})/F)$ et, pour tout $g \in G$, un représentant $a_g \in \mathbb{Z}$ 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 $\sigma_g \in \mathrm{Gal}(\mathbb{Q}(\zeta_{dp^n})/\mathbb{Q})$ le relèvement de g tel que $\zeta_{dp^n} = \zeta_{dp^n}^{\sigma_g a_g}$ alors on a $\zeta_{dp^n} = \zeta_{dp^n}^{a_g\sigma_g} \equiv \xi_\ell^{a_g(\ell-1)/dp^n}[\mathcal{L}(\lambda)^{\sigma_g}]$, parce que σ_g agit trivialement sur ξ_ℓ. On calcule maintenant $\phi_{\ell,n}(c^F(r))$:

$$\begin{aligned}
\phi_{\ell,n}(c^F(r)) &= \left(res_{\lambda^g}(\varphi_n(c^F(r)))\right)_{g\in G} \text{ par définition de } \phi_{\ell,n},\\
&= \left(red_{\lambda^g}(r-1)(\varphi_n(c^F(r)))\right)_{g\in G} \text{ voir diagramme (12)}\\
&= \left(red_{\lambda^g}(r-1)\left(\sum_\sigma \kappa^{r-1}(\sigma)\sigma(1-\zeta_{dp^n})\otimes t(r-1)_n\right)\right)_{g\in G}\\
&\text{par la formule (7) et où } \sigma \text{ parcourt } \mathrm{Gal}(\mathbb{Q}(\zeta_{dp^n})/F)\\
&= \left(red_{\lambda^g}(r-1)((\prod_{i\in I_{F,n}}(1-\zeta_{dp^n}^i)^{i^{r-1}})\otimes t(r-1)_n)\right)_{g\in G}\\
&= \left(\prod_{i\in I_{F,n}}(1-\xi_\ell^{a_g i(\ell-1)/(dp^n)})^{i^{r-1}}\otimes t(r-1)_n\right)_{g\in G}.
\end{aligned}$$

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

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

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

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

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

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

Démonstration. — Pour calculer l'indice

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

on commence par enlever les $r-1$ tordus à la Tate au numérateur et au dénominateur ce qui ne change pas l'indice. Ensuite si on prend $\eta_\ell = \xi_\ell$ on trouve d'après la

proposition 7.3 et le lemme 7.1 l'égalité

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

Clairement cette égalité reste valable avec tout choix de racine primitive modulo ℓ autre que ξ_ℓ parce que l'indice de gauche dans l'égalité (13) ne dépend 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 théorème 7.4. □

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

8. Quelques résultats numériques

Voici, suivant une des suggestions du referee, quelques exemples numériques obtenus avec le logiciel SAGE. Le code SAGE utilisé et d'autres données numériques sont disponible sur la page http ://www-irma.u-strasbg.fr/∼beliaeva/codes.html. Pour simplifier l'algorithme, tous les cas présentés ici concernent des corps de nombre de degré p. Pour ces corps il n'y a qu'un caractère non trivial à $\mathbb{Q}_p$-conjugaison près, d'où l'absence de variation en fonction du choix des caractères. On se restreint aussi à des corps de conducteur d premier avec $d \equiv 1[p]$, pour que $\mathbb{Q}(\zeta_d)$ contienne un unique sous-corps de degré p sur $\mathbb{Q}$. On note $F_{d,p}$ ce sous-corps de degré p de $\mathbb{Q}(\zeta_d)$. D'après le corollaires 6.7, pour $F = F_{d,p}$ on a :

$$\#\frac{H^1(G_S,\mathbb{Z}_p(r))^\chi}{\langle c^{F_{d,p}}(r)\rangle^\chi} = \min_{\ell\in\mathbb{L}'_1, n\le v_p(\ell-1)}\left\{\mathrm{ire}_{r,\chi,\ell,n};\ \mathrm{ire}_{r,\chi,\ell,n} < \mathrm{ima}_{\chi,n}\right\}.$$

On a donc calculé les $\mathrm{ire}_{r,\chi,\ell,n}$ pour $p = 3,5,7,11$ et $\ell < 10^6$. Cela donne une majoration de l'indice $\#\frac{H^1(G_S,\mathbb{Z}_p(r))^\chi}{\langle c^{F_{d,p}}(r)\rangle^\chi}$, mais au vu des résultats numériques on peut s'attendre à ce que le $\mathrm{ire}_{r,\chi,\ell,n}$ retenu soit égal à cet indice. En tout cas cela se produit chaque fois qu'un $\mathrm{ire}_{r,\chi,\ell,n}$ est égal à p.

En effet l'indice calculé $\#\frac{H^1(G_S,\mathbb{Z}_p(r))^\chi}{\langle c^F(r)\rangle^\chi}$ n'est jamais trivial à cause de la différence entre $C^F(r)$ et $\langle c^F(r)\rangle$. Concrètement, avec la relation (8) entre $c^F(r)$ et l'autre générateur $c_1^F(r)$ du module $C^F(r)$, on obtient que le quotient $C^F(r)/\langle c^F(r)\rangle$ est isomorphe à $\mathbb{Z}_p/(1-d^{r-1})\mathbb{Z}_p$ avec action triviale de G. Et comme $p \mid (1-d^{r-1})$, on trouve pour tout caractère χ non trivial sur G l'isomorphisme $(C^F(r)/\langle c^F(r)\rangle)^\chi \simeq \mathbb{Z}_p/p\mathbb{Z}_p$. En conséquence si on part de la suite $0 \longrightarrow \frac{C^F(r)}{\langle c^F(r)\rangle} \longrightarrow \frac{H^1(G_S,\mathbb{Z}_p(r))}{\langle c^F(r)\rangle} \longrightarrow \frac{H^1(G_S,\mathbb{Z}_p(r))}{C^F(r)} \longrightarrow 0$, on obtient en passant aux

χ-parties la suite $0 \longrightarrow \mathbb{Z}_p/p\mathbb{Z}_p \longrightarrow \frac{H^1(G_S,\mathbb{Z}_p(r))^\chi}{\langle c^F(r)\rangle^\chi} \longrightarrow \left(\frac{H^1(G_S,\mathbb{Z}_p(r))}{C^F(r)}\right)^\chi \longrightarrow \cdots$.
Ainsi dès que l'indice calculé $\mathrm{ire}_{r,\chi,\ell,n}$ est exactement p on sait que c'est aussi l'indice $\#\frac{H^1(G_S,\mathbb{Z}_p(r))^\chi}{\langle c^F(r)\rangle^\chi}$.

Pour chacun de ces corps on a testé les r-tordus à la Tate pour des r impairs allant de 3 à 21. Dans certains cas il n'y a pas de variation en fonction de r. Le même indice apparaît pour la première fois pour le même couple (ℓ, n).

Voici quelques exemples où le résultat des calculs effectués ne dépend pas de r ; dans tous ces cas on remarque que l'indice minimal apparaît pour le plus petit ℓ dans $\mathbb{L}_1'$:

1. $p = 3$, $d = 7$ ($F = F_{3,7} = \mathbb{Q}(\cos(\frac{2\pi}{7}))$: l'indice est 3, il apparaît pour la première fois pour $\ell = 43,\ n = 1$;
2. $p = 3$, $d = 13$ ($F = L_{3,13} = \mathbb{Q}(\cos(\frac{2\pi}{13}) + \cos(\frac{10\pi}{13}))$) : l'indice est 3, il apparaît pour la première fois pour $\ell = 79,\ n = 1$;
3. $p = 5$, $d = 11$ ($F = F_{5,11} = \mathbb{Q}(\cos(\frac{2\pi}{11}))$) : l'indice minimal trouvé est 5^3, il apparaît pour la première fois pour $\ell = 331,\ n = 1$;
4. $p = 5$, $d = 41$ ($F = F_{5,41} = \mathbb{Q}(\cos(\frac{2\pi}{41}) + \cos(\frac{3\pi}{41}) + \cos(\frac{9\pi}{41}) + \cos(\frac{14\pi}{41}))$: l'indice minimal trouvé est 5^3, il apparaît pour la première fois pour $\ell = 821,\ n = 1$;
5. $p = 7$, $d = 29$ ($F = F_{7,29}$) : l'indice minimal trouvé est 7^5, il apparaît pour la première fois pour $\ell = 2437,\ n = 1$;
6. $p = 7$, $d = 43$ ($F = F_{7,43}$) : l'indice minimal trouvé est 7^5, il apparaît pour la première fois pour $\ell = 3011,\ n = 1$;
7. $p = 11$, $d = 23$ ($F = F_{11,23}$) : l'indice minimal trouvé est 11^9, il apparaît pour la première fois pour $\ell = 1013,\ n = 1$.

Voici d'autres exemples où l'indice dépend de r :

p	d	r	indice	première apparition
3	19	3,5,9,11,15,17,21	3^3	$\ell = 2053,\ n = 2$
		7,13	3^5	$\ell = 2053,\ n = 3$
		19	3^7	$\ell = 3079,\ n = 4$
	37	3,5,9,11,15,17,21	3^5	$\ell = 1999,\ n = 3$
		7,13	3^7	$\ell = 41959,\ n = 4$
		19	3^9	$\ell = 161839,\ n = 5$
5	31	3,7,11,15,19	5^3	$\ell = 311,\ n = 1$
		5,9,13,17	5^7	$\ell = 4651,\ n = 2$
		21	5^{11}	$\ell = 23251,\ n = 3$

Dans les exemples traités pour $p = 7$ et $p = 11$ on n'a pas de variation en fonction de r.

Références

[1] A. A. Beĭlinson – « 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. Nguyên-Quang Dô – « 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 **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. Nguyên Quang Dô & 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.

[24] V. Voevodsky – « On motivic cohomology with $\mathbb{Z}/l$-coefficients », *Ann. of Math. (2)* **174** (2011), no. 1, p. 401–438.

---

11 décembre 2011

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