Algebra & Number Theory

Volume 5
2011
No. 6

Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques

Guillaume Perbet

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 5:6(2011)

Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques

Guillaume Perbet

Soit K_∞/K une extension infinie du corps de nombres K, dont le groupe de Galois G est un pro-p-groupe p-valué de type fini et dans laquelle seul un nombre fini de places sont ramifiées. La filtration entière de G fixe des étages finis K_n/K dans la tour K_∞/K. Pour deux ensembles finis S et T de places de K, on attache à K_n le groupe de Galois $X_{S,n}^T$ de sa pro-p-extension abélienne S-ramifiée et T-décomposée maximale, que la théorie du corps de classes interprète comme un groupe des classes généralisées. On démontre pour ces groupes des formules asymptotiques semblables à celle du théorème d'Iwasawa sur l'évolution du nombre de classes le long d'une $\mathbb{Z}_p$-extension. Les preuves utilisent les résultats de structure en théorie d'Iwasawa non-commutative et font apparaître les invariants d'Iwasawa attachés au module à l'infini $X_{S,\infty}^T$. Ces formules donnent des relations de dualité entre les invariants de $X_{S,\infty}^T$ et ceux de $X_{T,\infty}^S$, et débouchent sur des calculs d'invariants d'Iwasawa.

Let K_∞/K be an infinite extension of the number field K, with a p-valued pro–p-group of finite type G as Galois group, and such that only finitely many primes are ramified in this extension. The integral filtration on G fixes finite layers K_n/K in the tower K_∞/K. For S and T two finite sets of primes of K, one can attach to K_n the Galois group $X_{S,n}^T$ of his maximal S-ramified and T-split abelian pro–p-extension, which can be viewed as a generalized class group via class field theory. For these groups, we prove asymptotic formulas similar to Iwasawa's theorem on class numbers in $\mathbb{Z}_p$-extensions. The proofs use structure results in noncommutative Iwasawa theory and involve Iwasawa's invariants of the module at infinity $X_{S,\infty}^T$. These formulas give duality relations between invariants of $X_{S,\infty}^T$ and those of $X_{T,\infty}^S$, and lead to computations of Iwasawa invariants.

MSC2000: primary 11R23; secondary 11R29.

Mots-clefs: théorie d'Iwasawa non-commutative, invariants d'Iwasawa, extensions de Lie p-adiques, formules asymptotiques, noncommutative Iwasawa theory, Iwasawa invariants, p-adic Lie extensions, asymptotic formulas.

Introduction

Soit p un nombre premier et soit K un corps de nombres. Soit K_∞/K une $\mathbb{Z}_p$-extension, de groupe de Galois Γ. Dans les articles fondateurs de la théorie d'Iwasawa se trouve une formule asymptotique qui donne l'évolution du cardinal de la p-partie du groupe des classes le long de K_∞/K. Elle est donnée dans le théorème suivant, où X_n désigne la p-partie du groupe des classes du n-ième étage K_n de la tour K_∞/K :

Théorème (Iwasawa [Serre 1966, théorème 2]). *Il existe des entiers $\mu, \lambda \in \mathbb{N}$ et $\nu \in \mathbb{Z}$ ainsi qu'un rang n_0 tels que pour $n \geqslant n_0$*

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

La démonstration de ce résultat est évocatrice de l'efficacité des techniques de montée-descente, et du rôle central que joue l'algèbre d'Iwasawa $\Lambda(\Gamma) = \mathbb{Z}_p[\![\Gamma]\!]$. En effet, les constantes μ et λ sont des invariants algébriques attachés au Λ-module à l'infini X_∞, limite projective pour les applications norme des X_n. Ils proviennent d'un théorème de structure à pseudo-isomorphisme près pour les $\Lambda(\Gamma)$-modules de type fini (voir [Serre 1966]). Ce résultat a été étendu à des $\mathbb{Z}_p^d$ extensions par Cuoco et Monsky [1981].

Pour S et T deux ensembles finis disjoints de places de K, le théorème d'Iwasawa fut généralisé aux p-groupes des T-classes S-infinitésimales $X_{S,n}^T$ des corps K_n par Jaulent [1986; 2005]. La principale différence avec le groupe des classes classique vient du fait que $X_{S,n}^T$ n'est pas en général fini, ce qui entraîne l'apparition d'un invariant supplémentaire ρ. Il démontre :

Théorème [Jaulent 2005]. *Il existe des entiers ρ_S^T et μ_S^T tels que*

$$\#(X_{S,n}^T/p^n) = p^{\rho_S^T n p^n + \mu_S^T p^n + O(n)}.$$

Plus récemment, de nombreux auteurs se sont penchés sur une version non-commutative de la théorie d'Iwasawa. Les extensions infinies K_∞/K que l'on considère ont pour groupe de Galois un groupe de Lie p-adique G. Comme en théorie commutative, il est essentiel de bien connaître la structure des modules de type fini sur l'algèbre d'Iwasawa $\Lambda = \mathbb{Z}_p[\![G]\!]$. Même si l'on ne dispose pas d'un théorème de structure satisfaisant, des résultats partiels ont été obtenus par Venjakob [2002] et par Coates, Schneider et Sujatha [Coates et al. 2003]. Dans leurs travaux, ils introduisent une bonne notion de pseudo-nullité dans le cadre non-commutatif et ils définissent les invariants d'Iwasawa ρ et μ d'un Λ-module de type fini. On ajoute ici un troisième invariant, noté r, qui tout comme μ est attaché à la partie de $\mathbb{Z}_p$-torsion du Λ-module étudié (définition 1.4).

On propose, dans ce travail, de généraliser les formules asymptotiques sur le nombre de classes lorsque l'on monte dans une extension de Lie p-adique K_∞/K

dont le groupe de Galois G est un pro-p-groupe p-valué de type fini de dimension $d \geqslant 1$, et dans laquelle seul un nombre fini de places de K se ramifient.

On introduit la filtration entière G_n sur G, qui est une suite de sous-groupes d'indice Cp^{nd} pour n assez grand. On détermine alors l'évolution asymptotique des p-groupes des classes généralisées $X_{S,n}^T$ attachés aux sous-corps K_n, fixés par G_n.

Pour ce faire, on considère le Λ-module à l'infini $X_{S,\infty}^T = \varprojlim X_{S,n}^T$. Il est possible de redescendre à partir de ce module pour obtenir des informations sur les groupes $X_{S,n}^T$ (proposition 3.2). Notons $\rho_S^T, \mu_S^T, r_S^T \in \mathbb{N}$ les invariants d'Iwasawa de $X_{S,\infty}^T$. Cette technique de descente permet déjà de voir, utilisant un résultat de Harris, que l'invariant ρ_S^T contrôle l'évolution asymptotique du $\mathbb{Z}_p$-rang des $X_{S,n}^T$:

Théorème [Harris 2000, théorème 1.10].

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}^T) = \rho_S^T (G : G_n) + O(p^{n(d-1)}).$$

Cette formule conduit au calcul de l'invariant ρ_S^T lorsque K_∞/K contient la $\mathbb{Z}_p$-extension cyclotomique de K et que les étages sont totalement réels ou à multiplication complexe (CM) : voir théorème 3.14.

Pour dégager des résultats plus précis, faisant intervenir les invariants μ et r, on effectue une étude algébrique approfondie des Λ-modules. On arrive alors au résultat suivant :

Théorème 0.1. *On a*

$$\dim_{\mathbb{F}_p}(X_{S,n}^T/p) = (\rho_S^T + r_S^T)(G : G_n) + O(p^{n(d-1)})$$

et

$$\#(X_{S,n}^T/p^n) = p^{(\rho_S^T n + \mu_S^T)(G:G_n) + O(np^{n(d-1)})}.$$

A l'image de ce qui est fait par Jaulent et Maire [2003] dans le cas commutatif, ces résultats sont exploités à l'aide des formules de réflexion de Gras [1998]. Lorsque l'ensemble $S \cup T$ contient les places p-adiques Pl_p et en présence de racines de l'unité, on obtient une dualité entre décomposition et ramification qui prend la forme suivante :

Théorème 0.2. *Supposons que* $\mathrm{Pl}_p \subset S \cup T$, $\mu_p \subset K$ *et que* K_∞/K *contient la* $\mathbb{Z}_p$*-extension cyclotomique de* K*. Alors on a les identités*

$$\rho_S^T + \frac{\delta_T}{2} = \rho_T^S + \frac{\delta_S}{2}, \quad r_S^T = r_T^S \quad \textit{et} \quad \mu_S^T = \mu_T^S,$$

avec $\delta_S = \sum_{v \in S \cap \mathrm{Pl}_p} [K_v : \mathbb{Q}_p]$.

On énonce également des formules de ce type, sous l'hypothèse moins restrictive que K contient les racines p-ièmes de l'unité (théorèmes 3.8 pour $p = 2$ et 3.9 pour p impair). Elles rejoignent les formules de réflexion obtenues par Maire [2005] dans le cas commutatif.

La partie 1 est dédié à la présentation des invariants d'Iwasawa d'un Λ-module de type fini. On rappelle les principales propriétés des groupes p-valués, établies par Lazard [1965], ainsi que de leur algèbre d'Iwasawa Λ. On introduit alors les invariant d'Iwasawa ρ, μ et r d'un Λ-module de type fini, et on étudie leur comportement vis-à-vis des pseudo-isomorphismes.

La seconde partie, tout comme la première, est purement algébrique. Son but est la démonstration du théorème 2.1, qui indique qu'étant donné un Λ-module de type fini M, le comportement asymptotique de ses coïnvariants M_{G_n} est contrôlé par ses invariants d'Iwasawa. Les démonstrations utilisent fortement la notion de pseudo-nullité dans le cadre non-commutatif, introduite par Venjakob [2002], ainsi que les théorèmes de structure à pseudo-isomorphisme près dont on dispose (voir aussi [Coates et al. 2003]).

Ces résultats sont ensuite appliqués à un cadre arithmétique. On démontre des formules "à la Iwasawa" concernant l'évolution asymptotique des p-groupes des classes généralisés le long d'une extension d'un corps de nombres de groupe de Galois uniforme. On en déduit des résultats de dualité entre les invariants d'Iwasawa, lorsque l'on intervertit les conditions de ramification et de décomposition. Ces résultats permettent, dans certains cas, d'effectuer des calculs d'invariants ρ.

1. Sur les invariants d'Iwasawa

Groupes p-valués. Les groupes p-adiques analytiques, qui sont les groupes topologiques possédant une structure compatible de variété analytique sur $\mathbb{Q}_p$, sont au coeur de la théorie d'Iwasawa non-commutative. On va se focaliser, dans cette étude, sur une certaine classe de groupes analytiques possédant de bonnes propriétés : les pro-p-groupes p-valués de type fini. L'introduction de ces groupes et leur étude remontent à Lazard [1965]. Les propriétés exposées dans cette section proviennent de ses travaux.

Définition 1.1. Un groupe G est dit p-valué s'il est muni d'une application $\omega : G \to \mathbb{R}_+^* \cup \{+\infty\}$, appelée filtration, vérifiant les axiomes :

(i) $\omega(xy^{-1}) \geqslant \min(\omega(x), \omega(y))$,

(ii) $\omega(x^{-1}y^{-1}xy) \geqslant \omega(x) + \omega(y)$,

(iii) $\omega(x) = +\infty \iff x = 1$,

(iv) $\omega(x) > (p-1)^{-1}$,

(v) $\omega(x^p) = \omega(x) + 1$.

Proposition 1.2. *Soit G un groupe p-valué profini de type fini. Alors :*

(1) *Le groupe G est un pro-p-groupe analytique sans élément d'ordre fini.*

(2) *La filtration ω est discrète.*

On se donne dans la suite un pro-p-groupe p-valué de type fini G. On notera d sa dimension (en tant que groupe analytique), que l'on suppose supérieure à 1. On peut prendre un pro-p-groupe uniforme, pour la filtration induite par la suite centrale descendante (voir [Dixon et al. 1999]). Les exemples les plus classiques sont $\mathbb{Z}_p^d$ ou les sous-groupes de congruence des groupes linéaires $\mathrm{GL}_r(\mathbb{Z}_p)$.

On peut grossir la filtration initiale sur G en posant, pour $n \in \mathbb{N}^*$:

$$G_n = \{x \in G \mid \omega(x) > (p-1)^{-1} + n - 1\}.$$

La filtration induite par les sous-groupes G_n donne une structure de groupe p-valué sur G dont les valeurs sont entières.

Proposition 1.3. *Soit G un pro-p-groupe p-valué de type fini de dimension d et G_n les sous-groupes de G définis ci-dessus. Il existe une constante C telle que les indices des G_n dans G vérifient*

$$(G : G_n) = Cp^{nd}$$

pour n assez grand.

Démonstration. On utilise les résultats et le vocabulaire de [Lazard 1965].

Pour n_0 assez grand, le groupe G_{n_0} est p-saturé de dimension d [ibid., III 3.1.13]. En particulier, $(G_{n_0} : G_{n_0+k}) = p^{kd}$ [ibid., III 3.1.8] et on a pour $n \geqslant n_0$

$$(G : G_n) = (G : G_{n_0})(G_{n_0} : G_n) = p^{c+(n-n_0)d}. \qquad \square$$

Lorsque G est uniforme, on a $G_n = G^{p^n}$ et la constante C de la proposition 1.3 est égale à 1.

***L'algèbre d'Iwasawa* Λ.** On énonce dans ce paragraphe quelques propriétés vérifiées par l'algèbre d'Iwasawa d'un pro-p-groupe p-valué de type fini G, de dimension d.

On définit l'algèbre d'Iwasawa associée à G par

$$\Lambda(G) = \Lambda := \mathbb{Z}_p[\![G]\!] = \varprojlim_{U \lhd_o G} \mathbb{Z}_p[G/U],$$

où U parcout l'ensemble des sous-groupes distingués ouverts de G.

On sera aussi amené à considérer l'algèbre complète de G sur $\mathbb{F}_p$:

$$\Omega(G) = \Omega := \mathbb{F}_p[\![G]\!] = \varprojlim_{U \lhd_o G} \mathbb{F}_p[G/U].$$

Pour un sous-groupe U de G, on définit l'idéal d'augmentation I_U de Λ (ou de Ω) comme le noyau de la réduction modulo U.

Il est prouvé dans [Lazard 1965, II 2.2.2] que les algèbres Λ et Ω sont locales, d'idéaux maximaux respectifs $p\Lambda + I_G$ et I_G. Cette même référence nous informe que les algèbres graduées $\mathrm{Gr}(\Lambda) = \bigoplus I_{G_n}/I_{G_{n+1}}$ et $\mathrm{Gr}(\Omega)$ sont des algèbres de polynômes à respectivement $d+1$ et d variables [ibid., III 2.3.3]. En particulier, les algèbres Λ et Ω sont noethériennes à droite et à gauche et intègres.

Invariants des Λ-modules. Maintenant, Λ désignera l'algèbre d'Iwasawa d'un pro-p-groupe p-valué de type fini G. On s'intéresse alors aux Λ-modules de type fini, c'est-à-dire aux $\mathbb{Z}_p$-modules topologiques avec une action continue de G, qui sont de type fini pour leur structure de Λ-module étendant l'action de G. On va définir trois invariants pour de tels modules. Ils généralisent les invariants d'Iwasawa ρ, μ et r qui apparaissent dans le théorème de structure lorsque le groupe G est isomorphe à $\mathbb{Z}_p$, l'invariant r désignant le nombre de facteurs dans la partie de $\mathbb{Z}_p$-torsion. Les invariants ρ et μ ont déjà fait l'objet d'études de la part de Harris [1979], Venjakob [2002] et Howson [2002].

Définition 1.4. Soit M un Λ-module de type fini. Pour $i \in \mathbb{N}$ on note par $M[p^i]$ les éléments de M tués par p^i. On définit les invariants d'Iwasawa de M par

$$\begin{aligned}\rho(M) &= \mathrm{rk}_\Lambda(M) = \dim_F(F \otimes_\Lambda M),\\ r(M) &= \mathrm{rk}_\Omega(M[p]),\\ \mu(M) &= \sum_{i\geq 0} \mathrm{rk}_\Omega(M[p^{i+1}]/M[p^i]),\end{aligned}$$

avec F le corps gauche des fractions de Λ (voir [Lesieur et Croisot 1959]).

L'invariant ρ est le rang de M. Il est additif sur les suites exactes de Λ-modules et un Λ-module M est de torsion si et seulement si $\rho(M)=0$. Quant aux invariants r et μ, ils mesurent la $\mathbb{Z}_p$-torsion de M. L'invariant μ ne dépend que du sous-module de $\mathbb{Z}_p$-torsion de M et est additif sur les suites exactes de modules de Λ-torsion (voir [Venjakob 2002, corollaire 3.37]), tandis que r ne dépend que de $M[p]$ et est additif sur les suites exactes de modules tués par p. Ces deux derniers invariants sont aussi donnés par les formules suivantes :

Lemme 1.5. *Pour M un Λ-module de type fini, on a*

$$r(M) = \mathrm{rk}_\Omega(\mathrm{tor}_{\mathbb{Z}_p}(M)/p) = \mathrm{rk}_\Omega(\mathrm{tor}_\Lambda(M)/p),$$

$$\begin{aligned}\mu(M) &= \sum_{i\geq 0} \mathrm{rk}_\Omega(p^i\mathrm{tor}_{\mathbb{Z}_p}(M)/p^{i+1}\mathrm{tor}_{\mathbb{Z}_p}(M))\\ &= \sum_{i\geq 0} \mathrm{rk}_\Omega(p^i\mathrm{tor}_\Lambda(M)/p^{i+1}\mathrm{tor}_\Lambda(M)).\end{aligned}$$

Démonstration. Notons dans cette preuve $T = \mathrm{tor}_{\mathbb{Z}_p}(M)$. L'anneau Λ étant noethérien, il existe un entier α tel que $T = M[p^\alpha]$.

Quotienter par p la suite exacte

$$0 \to pT \to T \to T/p \to 0$$

conduit à la suite exacte de Ω-modules

$$0 \to (pT)[p] \to T[p] \to T/p \to (pT)/p \to T/p \to T/p \to 0.$$

La somme alternée des Ω-rangs nous informe que

$$\mathrm{rk}_\Omega(T[p]) - \mathrm{rk}_\Omega(T/p) = \mathrm{rk}_\Omega((pT)[p]) - \mathrm{rk}_\Omega((pT)/p).$$

Il est possible d'itérer les calculs en remplaçant T par pT. On obtient, pour tout entier i,

$$\mathrm{rk}_\Omega(T[p]) - \mathrm{rk}_\Omega(T/p) = \mathrm{rk}_\Omega((p^iT)[p]) - \mathrm{rk}_\Omega((p^iT)/p) = 0,$$

la nullité provenant du cas $i = \alpha$. On justifie la première égalité du lemme pour r et μ en notant que

$$T[p^{i+1}]/T[p^i] \simeq p^i(T[p^{i+1}]) = (p^iT)[p].$$

Enfin, pour voir que l'on peut calculer μ et r à partir du sous-module $\mathrm{tor}_\Lambda(M)$, on regarde pour tout $i \in \mathbb{N}$ la suite exacte

$$0 \to p^iT \to p^i\mathrm{tor}_\Lambda(M) \to p^i\mathrm{tor}_\Lambda(M)/p^iT \to 0.$$

Le dernier terme de cette suite, que l'on note N, est un Λ-module de torsion sans p-torsion. Quotienter par p donne donc

$$0 \to p^iT/p^{i+1}T \to p^i\mathrm{tor}_\Lambda(M)/p^{i+1}\mathrm{tor}_\Lambda(M) \to N/p \to 0,$$

où N/p est un Ω-module de torsion. L'additivité du rang permet de conclure que

$$\mathrm{rk}_\Omega(p^iT/p^{i+1}T) = \mathrm{rk}_\Omega(p^i\mathrm{tor}_\Lambda(M)/p^{i+1}\mathrm{tor}_\Lambda(M)). \qquad \square$$

Pseudo-nullité et invariants. Beaucoup de résultats de la théorie d'Iwasawa classique, lorsque $G \simeq \mathbb{Z}_p$, reposent sur le théorème de structure des Λ-modules de type fini à pseudo-isomorphisme près (voir par exemple [Serre 1966]). Coates et al. [2003], ainsi que Venjakob [2002], ont ouvert la voie vers une généralisation au cas non-commutatif de ce théorème. On rappelle la notion de pseudo-nullité qu'ils ont introduite dans ce contexte. La notation $\mathrm{Ext}_\Lambda(-,-)$ désignera les dérivés du bifoncteur $\mathrm{Hom}_\Lambda(-,-)$ des homomorphismes continus entre Λ-modules de type fini.

Définition 1.6. Un Λ-module de type fini M est dit pseudo-nul si

$$\mathrm{Ext}^0_\Lambda(M,\Lambda) = \mathrm{Ext}^1_\Lambda(M,\Lambda) = 0.$$

Un morphisme $f : M \to N$ entre deux Λ-modules de type fini est appelé pseudo-isomorphisme si le noyau et le conoyau de f sont pseudo-nuls.

Le lemme suivant indique que la sous-catégorie des modules pseudo-nuls vérifie la condition de Serre et permet de considérer la catégorie quotient.

Lemme 1.7. *Tout sous-module et tout quotient d'un module pseudo-nul est pseudo-nul.*

Démonstration. C'est la proposition 3.6 de [Venjakob 2002]. □

On démontre alors la proposition suivante, qui met en évidence le fait que les invariants d'Iwasawa se comportent bien vis-à-vis des pseudo-isomorphismes.

Proposition 1.8. *Soit M et N deux Λ-modules de type fini pseudo-isomorphes. Alors $\rho(M) = \rho(N)$, $\mu(M) = \mu(N)$ et $r(M) = r(N)$.*

Démonstration. La condition $\mathrm{Ext}^0_\Lambda(A, \Lambda) = \mathrm{Hom}_\Lambda(A, \Lambda) = 0$ indique que tout Λ-module pseudo-nul A est de torsion. Ceci entraîne que $\rho(A) = 0$ et, comme ρ est aussi additif sur les suites exactes, il est invariant modulo pseudo-isomorphisme.

En ce qui concerne r, on écrit la suite exacte donnée par le pseudo-isomorphisme

$$0 \to A \to M \xrightarrow{f} N \to B \to 0$$

et on note $Z = \mathrm{Im}(f)$. Le lemme du serpent permet d'extraire les deux suites exactes

$$A[p] \to M[p] \to Z[p] \to A/p \quad \text{et} \quad 0 \to Z[p] \to N[p] \to B[p].$$

D'après le lemme 1.7, les termes extrémaux de ces deux suites sont des modules pseudo-nuls tués par p. Le lemme 1.9 ci-dessous donne alors $r(M) = r(Z) = r(N)$ en regardant les Ω-rangs des termes des deux suites.

Lemme 1.9. *Si A est un Λ-module pseudo-nul tué par p, alors A est un Ω-module de torsion.*

Démonstration. Soit A un Λ-module pseudo-nul tué par p. La suite exacte

$$0 \to \Lambda \xrightarrow{p} \Lambda \to \Omega \to 0$$

conduit à l'encadrement

$$\mathrm{Ext}^0_\Lambda(A, \Lambda) \to \mathrm{Hom}_\Lambda(A, \Omega) \to \mathrm{Ext}^1_\Lambda(A, \Lambda).$$

La pseudo-nullité de A entraîne la nullité de $\mathrm{Hom}_\Lambda(A, \Omega)$, qui coïncide avec $\mathrm{Hom}_\Omega(A, \Omega)$. Le Ω-module A est donc de torsion. □

En ce qui concerne μ, on utilise des arguments similaires exposés dans la preuve de la proposition 3.34 de [Venjakob 2002]. □

On conclut ce paragraphe par un théorème qui donne la structure, à pseudo-isomorphisme près, de la $\mathbb{Z}_p$-torsion d'un Λ-module de type fini. Il permet, comme dans le cadre de la théorie commutative, de lire les invariants μ et r sur un module élémentaire.

Théorème 1.10 [Venjakob 2002, théorème 3.40]. *Soit M un Λ-module de type fini. Il existe des uniques entiers naturels $\alpha_1, \ldots, \alpha_r$ tels que l'on ait un pseudo-isomorphisme*

$$\mathrm{tor}_{\mathbb{Z}_p}(M) \to \bigoplus_{i=1}^{r} \Lambda/p^{\alpha_i}.$$

De plus, $r(M) = r$ et $\mu(M) = \sum_{i=1}^{r} \alpha_i$.

2. Comportement asymptotique des coïnvariants

On se donne G un pro-p-groupe p-valué de type fini de dimension $d \geqslant 1$. On le munit de sa filtration entière $(G_n)_n$ (voir page 823), et on pose $\Lambda = \mathbb{Z}_p[\![G]\!]$. Pour M un Λ-module de type fini, on notera M_{G_n} le plus grand quotient du module M sur lequel G_n agit trivialement. C'est le module des coïnvariants de M, qui s'obtient comme quotient

$$M_{G_n} = M/I_{G_n}M \simeq M \hat{\otimes}_{\Lambda(G_n)} \mathbb{Z}_p,$$

où $\hat{\otimes}_{\Lambda(G_n)}$ désigne le produit tensoriel complété (voir [Brumer 1966, section 2]).

Si G est isomorphe à $\mathbb{Z}_p$, le contenu de [Jaulent 2005], permet de voir que les invariants d'Iwasawa de M sont reliés aux cardinaux de certains quotients finis de ses coïnvariants. C'est ce type de résultats que l'on voudrait étendre à des extensions de groupe de Galois p-valué. Plus précisément, on démontre les deux résultats suivants :

Théorème 2.1. *Soit M un Λ-module de type fini d'invariants ρ, μ et r. Alors* :

(i) $\dim_{\mathbb{F}_p}(M_{G_n}/p) = (\rho + r)(G : G_n) + O(p^{n(d-1)})$.

(ii) $\#(M_{G_n}/p^n) = p^{(\rho n + \mu)(G:G_n) + O(np^{n(d-1)})}$.

Rappelons que $(G : G_n) = Cp^{nd}$ pour n assez grand, avec $C = 1$ si G est uniforme.

Un théorème de Harris. Le point de départ de la preuve du théorème 2.1 est un résultat de Harris [2000, théorème 1.10], que l'on formule de la façon suivante :

Théorème 2.2. *Si M est un Ω-module de type fini, alors*

$$\dim_{\mathbb{F}_p}(M_{G_n}) = \mathrm{rk}_\Omega(M)(G : G_n) + O(p^{n(d-1)}).$$

Démonstration. Pour M de Ω-torsion, les arguments de la preuve du théorème 1.10 de [Harris 2000] s'adaptent à un groupe p-valué et permettent de voir que $\dim_{\mathbb{F}_p}(M_{G_n}) = O(p^{n(d-1)})$.

Dans le cas général, on dévisse pour se ramener d'abord à un Ω-module sans torsion, puis à un Ω-module libre. □

Pour i et n des entiers naturels, les groupes d'homologie de G_n à coefficients dans un Λ-module de type fini M sont définis par

$$H_i(G_n, M) = \mathrm{Tor}_i^{\Lambda(G_n)}(\mathbb{Z}_p, M),$$

où $\mathrm{Tor}_i^{\Lambda(G_n)}(-,-)$ désignent les dérivés du bifoncteur $-\hat{\otimes}_{\Lambda(G_n)}-$.

Lorsque M est aussi muni d'une structure de Ω-module, le théorème 2.2 donne des renseignements sur $H_0(G_n, M) = M_{G_n}$. En effet, on a dans ce cas

$$H_i(G_n, M) = \mathrm{Tor}_i^{\Lambda(G_n)}(\mathbb{Z}_p, M) \simeq \mathrm{Tor}_i^{\Omega(G_n)}(\mathbb{F}_p, M)$$

(voir [Ribes et Zalesskii 2000, lemme 6.3.5]).

Le corollaire suivant étend le théorème 2.2 aux groupes d'homologie supérieurs pour les Ω-modules de torsion.

Corollaire 2.3. *Soit M un Ω-module de type fini et de torsion. Pour tout $i \geqslant 0$, on a*

$$\dim_{\mathbb{F}_p}(H_i(G_n, M)) = O(p^{n(d-1)}).$$

Démonstration. On procède par récurrence sur i, le cas $i = 0$ étant donné par le théorème 2.2.

Le Ω-module M étant de type fini et de torsion, il existe un Ω-module de torsion A et des éléments non nuls $f_1, \ldots, f_r \in \Omega$ prenant place dans la suite exacte

$$0 \to A \to \bigoplus_j \Omega/f_j \to M \to 0.$$

Cette suite conduit à l'encadrement

$$H_i(G_n, \bigoplus_j \Omega/f_j) \to H_i(G_n, M) \to H_{i-1}(G_n, A).$$

L'hypothèse de récurrence appliquée à A entraîne

$$\dim_{\mathbb{F}_p}(H_{i-1}(G_n, A)) = O(p^{n(d-1)})$$

et permet de se ramener au cas $M = \Omega/f$.

On calcule les groupes d'homologie de Ω/f à partir de sa résolution $\Omega(G_n)$-libre

$$0 \to \Omega \xrightarrow{f} \Omega \to \Omega/f \to 0.$$

On obtient immédiatement $H_i(G_n, \Omega/f) = 0$ pour $i > 1$, ainsi que les renseignements suivants sur le H_1 :

$$\begin{aligned}\dim_{\mathbb{F}_p}(H_1(G_n, \Omega/f)) &= \dim_{\mathbb{F}_p}(\ker(\Omega_{G_n} \xrightarrow{f} \Omega_{G_n}))\\ &= \dim_{\mathbb{F}_p}(\operatorname{coker}(\Omega_{G_n} \xrightarrow{f} \Omega_{G_n}))\\ &= \dim_{\mathbb{F}_p}((\Omega/f)_{G_n}) = O(p^{n(d-1)}),\end{aligned}$$

la dernière égalité provenant du théorème 2.2. □

On termine ce paragraphe par une dernière variante du théorème de Harris.

Corollaire 2.4. *Soit M un Λ-module de type fini tel que M/p est un Ω-module de torsion. Alors, pour tout $i \geqslant 0$,*

$$\#(H_i(G_n, M/p^n)) = p^{O(np^{n(d-1)})}.$$

Démonstration. On va découper M/p^nM selon les $p^kM/p^{k+1}M$. Le corollaire 2.3 fournit des constantes C_k, indépendantes de n, telles que

$$\#H_i(G_n, p^kM/p^{k+1}M) \leqslant p^{C_k p^{n(d-1)}}.$$

Pour $k < n$, la G_n-homologie de la suite exacte

$$0 \to p^{k+1}M/p^nM \to p^kM/p^nM \to p^kM/p^{k+1}M \to 0$$

entraîne les inégalités

$$\#H_i(G_n, p^kM/p^nM) \leqslant \#H_i(G_n, p^{k+1}M/p^nM)\, p^{C_k p^{n(d-1)}}.$$

Elles conduisent finalement à

$$\#H_i(G_n, M/p^nM) \leqslant p^{(C_1+\cdots+C_n)p^{n(d-1)}}.$$

Pour k assez grand, le module p^kM est sans p-torsion. Ainsi

$$p^kM/p^{k+1}M \simeq p^{k+1}M/p^{k+2}M$$

et les constantes C_k sont majorées par une constante C' indépendante de k. On en tire

$$\#H_i(G_n, M/p^nM) \leqslant p^{C'np^{n(d-1)}}.$$ □

Preuve du théorème 2.1 i). Pour un Λ-module M de type fini, on cherche à déterminer l'évolution asymptotique de $\dim_{\mathbb{F}_p}(M_{G_n}/p)$. Le théorème 2.2 appliqué à M/p donne l'estimation

$$\dim_{\mathbb{F}_p}(M_{G_n}/p) = \mathrm{rk}_\Omega(M/p)(G : G_n) + O(p^{n(d-1)}).$$

Le corollaire 1.10 de [Howson 2002] relie la valeur de $\mathrm{rk}_\Omega(M/p)$ aux invariants d'Iwasawa de M de la façon suivante :

$$\mathrm{rk}_\Omega(M/p) = \mathrm{rk}_\Omega(M[p]) + \mathrm{rk}_\Lambda(M) = r + \rho.$$

La combinaison de ces deux résultats donne la première formule du théorème 2.1.

Preuve du théorème 2.1 ii). Soit M un Λ-module de type fini. Pour démontrer le deuxième point du théorème 2.1, on va utiliser des résultats de structure modulo pseudo-isomorphisme pour M. Notons que les techniques de cette section fournissent également une preuve du point i) du théorème.

On commence par remarquer que la quantité $\#(M_{G_n}/p^n)$ que l'on veut calculer passe bien modulo pseudo-isomorphisme :

Proposition 2.5. *Soient M et N deux Λ-modules de type fini pseudo-isomorphes. Alors*

$$\#(M_{G_n}/p^n) = \#(N_{G_n}/p^n)\, p^{O(np^{n(d-1)})}.$$

Démonstration. Soit

$$0 \to A \to M \xrightarrow{f} N \to B \to 0$$

la suite exacte donnée par le pseudo-isomorphisme et soit $Z = \mathrm{Im}(f)$. On en déduit par passage au quotient les suites exactes

$$A_{G_n}/p^n \to M_{G_n}/p^n \to Z_{G_n}/p^n \to 0$$

et

$$\begin{tikzcd} B[p^n] \arrow[r] & Z/p^n \arrow[rr, "\varphi"] \arrow[dr, two heads] & & N/p^n \arrow[r] & B/p^n \arrow[r] & 0. \\ & & \mathrm{Im}(\varphi) \arrow[ur, hook] & & & \end{tikzcd}$$

Cette dernière se découpe pour donner

$$B[p^n]_{G_n} \to Z_{G_n}/p^n \to \mathrm{Im}(\varphi)_{G_n} \to 0$$

et

$$H_1(G_n, B/p^n) \to \mathrm{Im}(\varphi)_{G_n} \to N_{G_n}/p^n \to B_{G_n}/p^n \to 0.$$

Le lemme 1.9 permet d'appliquer le corollaire 2.4 à tout module pseudo-nul. Ceci fournit successivement :

$$\begin{aligned}\#(M_{G_n}/p^n) &= \#(Z_{G_n}/p^n)\,p^{O(np^{n(d-1)})}\\ &= \#(\mathrm{Im}(\varphi))\,p^{O(np^{n(d-1)})} = \#(N_{G_n}/p^n)\,p^{O(np^{n(d-1)})}.\end{aligned}$$ □

La première étape consite à séparer l'étude des Λ-modules de torsion de celle des Λ-modules sans torsion. On considère la catégorie quotient des Λ-modules de type fini par la sous-catégorie des modules pseudo-nuls (lemme 1.7) et on note Q le foncteur canonique de passage au quotient. On dispose du résultat de structure suivant :

Proposition 2.6 [Coates et al. 2003, proposition 6.4]. *Soit M un Λ-module de type fini. On a un isomorphisme dans la catégorie quotient* :

$$Q(M) \simeq Q(\mathrm{tor}_\Lambda(M)) \oplus Q(\widetilde{M}),$$

où $\widetilde{M}$ désigne le quotient de M par son sous-module de Λ-torsion.

Remarquons que $\mathrm{tor}_\Lambda(M)$ est un Λ-module de torsion dont les invariants μ et r sont égaux à ceux de M, tandis que $\widetilde{M}$ est un Λ-module sans torsion de même rang que M. Le corollaire suivant permet d'étudier $\mathrm{tor}_\Lambda(M)$ d'une part et $\widetilde{M}$ d'autre part.

Corollaire 2.7. *Avec les notations de la proposition précédente, on a* :

$$\#(M_{G_n}/p^n) = \#(\mathrm{tor}_\Lambda(M)_{G_n}/p^n)\#(\widetilde{M}_{G_n}/p^n)\,p^{O(np^{n(d-1)})}.$$

Démonstration. L'isomorphisme dans la catégorie quotient qui apparaît dans la proposition 2.6 signifie qu'il existe des modules pseudo-nuls A, B, C et un sous-module M' de M, avec M/M' pseudo-nul, prenant place dans le diagramme suivant (voir [Gabriel 1962, chapitre III]) :

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 & & \\
0 \arrow[r] & A \arrow[r] & M' \arrow[r] \arrow[d] & (\mathrm{tor}_\Lambda(M)\oplus\widetilde{M})/C \arrow[r] \arrow[u] & B \arrow[r] & 0 \\
 & & M \arrow[d] & \mathrm{tor}_\Lambda(M)\oplus\widetilde{M} \arrow[u] & & \\
 & & M/M' \arrow[d] & C \arrow[u] & & \\
 & & 0 & 0 \arrow[u] & &
\end{tikzcd}$$

On a donc des pseudo-isomorphismes entre M' et M, entre M' et $(\mathrm{tor}_\Lambda(M)\oplus\widetilde{M})/C$ et entre $\mathrm{tor}_\Lambda(M)\oplus\widetilde{M}$ et $(\mathrm{tor}_\Lambda(M)\oplus\widetilde{M})/C$. On applique alors la proposition 2.5 pour obtenir :

$$\begin{aligned}\#(M_{G_n}/p^n) &= \#(M'_{G_n}/p^n)\,p^{O(np^{n(d-1)})}\\ &= \#((\mathrm{tor}_\Lambda(M)\oplus\widetilde{M}/C)_{G_n}/p^n)\,p^{O(np^{n(d-1)})}\\ &= \#((\mathrm{tor}_\Lambda(M)\oplus\widetilde{M})_{G_n}/p^n)\,p^{O(np^{n(d-1)})}\\ &= \#(\mathrm{tor}_\Lambda(M)_{G_n}/p^n)\,\#(\widetilde{M}_{G_n}/p^n)\,p^{O(np^{n(d-1)})}.\end{aligned}$$ □

On détermine, dans le lemme suivant, la quantité $\#(\mathrm{tor}_\Lambda(M)_{G_n}/p^n)$.

Lemme 2.8. *Soit T un Λ-module de type fini, de torsion et d'invariant μ. Alors*

$$\#(T_{G_n}/p^n) = p^{\mu(G:G_n)+O(np^{n(d-1)})}.$$

Démonstration. On dévisse le problème en s'intéressant à la suite exacte

$$0\to \mathrm{tor}_{\mathbb{Z}_p}(T)\to T\to \overline{T}\to 0,$$

où $\overline{T}=T/\mathrm{tor}_{\mathbb{Z}_p}(M)$ est un module de Λ-torsion sans $\mathbb{Z}_p$-torsion. Le module $\overline{T}$ étant sans $\mathbb{Z}_p$-torsion, quotienter par p^n conserve l'exactitude de cette suite et conduit à la suite exacte d'homologie

$$H_1(G_n,\overline{T}/p^n)\to \mathrm{tor}_{\mathbb{Z}_p}(T)_{G_n}/p^n\to T_{G_n}/p^n\to \overline{T}_{G_n}/p^n\to 0.$$

Le corollaire 2.4, appliqué au module $\overline{T}$, permet d'obtenir la relation

$$\#(T_{G_n}/p^n) = \#(\mathrm{tor}_{\mathbb{Z}_p}(T)_{G_n}/p^n)\,p^{O(np^{n(d-1)})}.$$

Il suffit donc de contôler le cardinal de $\mathrm{tor}_{\mathbb{Z}_p}(T)_{G_n}/p^n$ à l'aide du théorème 1.10, qui fournit un pseudo-isomorphisme

$$\mathrm{tor}_{\mathbb{Z}_p}(T)\to\bigoplus_{i=1}^{r}\Lambda/p^{\alpha_i},$$

avec $\mu=\sum\alpha_i$. La proposition 2.5 nous informe alors que

$$\begin{aligned}\#(\mathrm{tor}_{\mathbb{Z}_p}(T)_{G_n}/p^n) &= \#\left(\bigoplus_{i=1}^{r}\mathbb{Z}_p[G/G_n]/(p^{\alpha_i},\,p^n)\right)p^{O(np^{n(d-1)})}\\ &= p^{\mu(G:G_n)+O(np^{n(d-1)})}.\end{aligned}$$ □

Il reste à évaluer la quantité $\#(\widetilde{M}_{G_n}/p^n)$. C'est l'objet du lemme :

Lemme 2.9. *Soit M un Λ-module de type fini, sans-torsion et de rang ρ. Alors*

$$\#(M_{G_n}/p^n) = p^{\rho n(G:G_n)+O(np^{n(d-1)})}.$$

Démonstration. Tout Λ-module sans torsion est contenu dans un module libre de même rang. On a donc une suite exacte

$$0 \to M \to \Lambda^{\rho} \to T \to 0,$$

qui conduit à la suite exacte de Ω-modules

$$0 \to T[p] \to M/p \to \Omega^{\rho} \to T/p \to 0.$$

La somme alternée des Ω-rangs nous informe que $r(M/p) = \rho$.

Le théorème 2.1 i) appliqué au Λ-module de torsion M/p donne alors une suite bornée $(c_n)_n$ telle que

$$\dim_{\mathbb{F}_p}(M_{G_n}/p) = \rho(G : G_n) + c_n p^{n(d-1)}.$$

Pour calculer $\#(M_{G_n}/p^n)$, on remarque que l'on a les isomorphismes suivants, du fait que M est sans torsion :

$$p^i : M/pM \xrightarrow{\sim} p^i M/p^{i+1}M.$$

On a ainsi

$$\begin{aligned}\#(M_{G_n}/p^n) &= \prod_{i=0}^{n} \#(p^i M/p^{i+1}M)_{G_n} \\ &= (\#(M_{G_n}/p))^n \\ &= p^{\rho n(G:G_n)+c_n n p^{n(d-1)}} \\ &= p^{\rho n(G:G_n)+O(np^{n(d-1)})}.\end{aligned}$$ □

La combinaison du corollaire 2.7 et des lemmes 2.8 et 2.9 fournit une preuve du théorème 2.1 ii).

3. Applications arithmétiques

On va appliquer les résultats de la partie 2 à une situation arithmétique faisant intervenir naturellement des Λ-modules. Plus précisément, on va étudier les invariants associés aux groupes de Galois de pro-p-extensions abéliennes maximales avec des conditions de ramification restreinte et de décomposition.

Le contexte arithmétique. On se fixe un corps de nombres K, qui fera office de corps de base. Soit K_∞/K une extension galoisienne vérifiant les hypothèses suivantes :

- Le groupe $G = \mathrm{Gal}(K_\infty/K)$ est un pro-p-groupe p-valué de type fini de dimension $d \geqslant 1$.
- Il n'y a qu'un nombre fini de places de K ramifiées dans K_∞/K.

L'exemple historique est celui des $\mathbb{Z}_p$-extensions et $\mathbb{Z}_p$-extensions multiples, qui sont abéliennes. Un exemple avec G non-commutatif est la fausse courbe de Tate, donnée par l'extension $\mathbb{Q}(\zeta_{p^\infty}, \sqrt[p^\infty]{p})/\mathbb{Q}(\zeta_p)$. Son groupe de Galois est isomorphe à un produit semi-direct $\mathbb{Z}_p \rtimes \mathbb{Z}_p$. Dans ces deux premières illustrations, seules les places au-dessus de p sont ramifiées.

On obtient aussi de telles extensions en regardant l'action du groupe de Galois absolu $G_K = \mathrm{Gal}(\overline{K}/K)$ sur les objets géométriques $H^i_{et}(\overline{Y}, \mathbb{Q}_p)(j)$, où Y est une variété projective lisse absolument irréductible définie sur K. Lorsque Y est une courbe elliptique non CM fixée, on réalise ainsi des $\mathrm{GL}_2(\mathbb{Z}_p)$-extension, à part pour un nombre fini de premiers p. Ces extensions sont non-ramifiées en dehors de p et des places de mauvaise réduction de Y (voir [Serre 1972]).

C'est dans ce contexte que l'on fait intervenir les Λ-modules d'Iwasawa. Soient S et T deux ensembles finis disjoints de places de K. On écrira encore, si aucune confusion n'est possible, S et T pour les places d'une extension L de K qui sont au-dessus de celles de S et T.

Soit H_S^T la pro-p-extension abélienne S-ramifiée et T-décomposée maximale de K_∞. On note $X_{S,\infty}^T = \mathrm{Gal}(H_S^T/K_\infty)$. On rappelle que S-ramifiée et T-décomposée signifie que seules les places de S peuvent se ramifier dans cette extension et que les places de T sont totalement décomposées. Pour une place infinie, "ramification" signifiera "complexification", tandis que "décomposition" sera synonyme de "non-complexification". Par maximalité de H_S^T/K_∞, l'extension H_S^T/K est galoisienne et on obtient une action de G sur $X_{S,\infty}^T$ par conjugaison, qui induit une structure de Λ-module sur $X_{S,\infty}^T$.

On munit G de sa filtation entière par les sous-groupes G_n (voir page 822) et note K_n le sous-corps de K_∞ fixé par G_n. On introduit aussi $\mathcal{G} = \mathrm{Gal}(H_S^T/K)$ et $\mathcal{G}_n = \mathrm{Gal}(H_S^T/K_n)$. Les notations prennent place dans le treillis suivant :

$$
\begin{tikzcd}
 & H_S^T \arrow[dl, dash] \arrow[dl, dash, bend right, "X_{S,\infty}^T"'] \arrow[ddl, dash, bend left, "\mathcal{G}_n"] \arrow[dddl, dash, bend left=60, "\mathcal{G}"] \\
K_\infty \arrow[d, dash] \arrow[d, dash, bend left, "G_n"] \arrow[dd, dash, bend right=60, "G"'] & \\
K_n \arrow[d, dash] & \\
K &
\end{tikzcd}
$$

Un autre moyen de récupérer le module $X^T_{S,\infty}$ est de le construire par limite projective. Pour tout n, on va désigner par $X^T_{S,n}$ le groupe de Galois de la pro-p-extension abélienne S-ramifiée et T-décomposée maximale de K_n. Le groupe $X^T_{S,\infty}$ se retrouve alors comme la limite projective des $X^T_{S,n}$ pour les applications de restriction. Chaque $X^T_{S,n}$ étant muni d'une structure de $\mathbb{Z}_p[G/G_n]$-module, compatible avec les applications de restriction, la structure de Λ-module de $X^T_{S,\infty}$ est héritée de cette construction.

La proposition suivante autorise à introduire les invariants ρ^T_S, μ^T_S et r^T_S du module d'Iwasawa $X^T_{S,\infty}$ (voir définition 1.4). On parlera aussi d'invariants de l'extension K_∞/K.

Proposition 3.1. *Le Λ-module $X^T_{S,\infty}$ est de type fini.*

Démonstration. Le résultat peut se voir sur le diagramme du lemme 4.3 de [Jannsen 1989] mais on en donne une preuve plus directe ici. On oublie les indices S et T dans cette preuve.

On obtient la suite exacte

$$H_2(G,\mathbb{F}_p) \to H_1(X_\infty,\mathbb{F}_p)_G \to H_1(\mathcal{G},\mathbb{F}_p)$$

en appliquant la suite exacte d'inflation-restriction à coefficients dans $\mathbb{F}_p$ à la suite exacte $0 \to X_\infty \to \mathcal{G} \to G \to 0$.

Le groupe abélien $H_2(G,\mathbb{F}_p)$ est de type fini du fait que G est analytique. Ce terme de gauche étant également tué par p, il est fini. Concernant le terme de droite, l'extension H^T_S/K est non-ramifiée en dehors de l'ensemble fini Σ, composé des places de S et des places ramifiées dans K_∞/K. Le groupe $\mathcal{G}$ est donc un quotient de G_Σ : groupe de Galois de la pro-p-extension maximale de K qui est non-ramifiée en dehors des places de Σ. D'après la théorie du corps de classes G_Σ est de type fini donc $\mathcal{G}$ aussi. Le terme de droite est ainsi lui aussi fini et on en déduit que le terme médian, $(X_\infty)_G/p$, est fini. D'après le lemme de Nakayama (voir [Balister et Howson 1997]), X_∞ est de type fini sur Λ. □

Les formules asymptotiques. La théorie du corps de classes interprète le module $X^T_{S,n}$ comme le p-groupe des T-classes S-infinitésimales de K_n (voir [Jaulent 1986]). Le module $X^T_{S,\infty}$ étant construit à partir des $X^T_{S,n}$, on retrouve des informations sur les groupes des classes généralisées à l'étage n à partir du module à l'infini. C'est le principe de montée-descente de la théorie d'Iwasawa.

Lorsque $G \simeq \mathbb{Z}_p$, $S = \varnothing$ et T est l'ensemble des places réelles de K, ce procédé donne l'un des tous premiers résultats d'Iwasawa dans son étude des $\mathbb{Z}_p$-extensions. Il obtient l'évolution asymptotique du nombre de p-classes le long d'une $\mathbb{Z}_p$-extension de corps de nombres et fait intervenir les invariants d'Iwasawa du module à l'infini correspondant (voir [Serre 1966]). Ce résultat a été, par la suite, généralisé par Jaulent au cas des p-groupes des T-classes S-infinitésimales, toujours le long d'une $\mathbb{Z}_p$-extension de corps de nombres [Jaulent 2005].

Dans le cas d'un groupe p-valué, le résultat suivant réalise la descente de $X^T_{S,\infty}$ à $X^T_{S,n}$. Il nous informe que le comportement asymptotique des G_n-coïnvariants $(X^T_{S,\infty})_{G_n}$ de $X^T_{S,\infty}$ est proche de celui des $X^T_{S,n}$.

Proposition 3.2. *On a*

$$\begin{aligned}\#((X^T_{S,\infty})_{G_n}/p^n) &= \#(X^T_{S,n}/p^n)\,p^{O(np^{n(d-1)})},\\ \dim_{\mathbb{F}_p}((X^T_{S,\infty})_{G_n}/p) &= \dim_{\mathbb{F}_p}(X^T_{S,n}/p) + O(p^{n(d-1)}),\\ \mathrm{rk}_{\mathbb{Z}_p}(X^T_{S,\infty})_{G_n} &= \mathrm{rk}_{\mathbb{Z}_p}(X^T_{S,n}) + O(p^{n(d-1)}).\end{aligned}$$

Démonstration. On oublie les indices S et T dans cette preuve et on se concentre sur la première équivalence.

La suite exacte d'inflation-restriction à coefficients dans $\mathbb{Z}/p^n\mathbb{Z}$, appliquée à la suite exacte

$$0 \to X_\infty \to \mathcal{G}_n \to G_n \to 0,$$

conduit à

$$H_2(G_n, \mathbb{Z}/p^n\mathbb{Z}) \to (X_\infty)_{G_n}/p^n \to \mathcal{G}_n^{ab}/p^n \to H_1(G_n, \mathbb{Z}/p^n\mathbb{Z}) \to 0.$$

Le corollaire 2.4 appliqué à $M=\mathbb{Z}_p$ nous indique que le cardinal de $H_i(G_n, \mathbb{Z}/p^n\mathbb{Z})$ évolue en $p^{O(np^{n(d-1)})}$. On en déduit que

$$\#((X_\infty)_{G_n}/p^n) = \#(\mathcal{G}_n^{ab}/p^n)\,p^{O(np^{n(d-1)})}.$$

Il reste donc à comparer $\mathcal{G}_n^{ab}$ à X_n. On s'appuie sur ce qui est fait dans le théorème 13.13 de [Washington 1997] pour $G \simeq \mathbb{Z}_p$, $S=\varnothing$ et T l'ensemble des places réelles de K.

La situation galoisienne nous informe que X_n s'obtient comme le quotient de $\mathcal{G}_n^{ab}$ par son sous-groupe $\mathcal{D}_n$, engendré par l'inertie des places hors de S et la décomposition des places de T. Soit D_{v_n} l'un des sous-groupes d'inertie ou de décomposition non triviaux qui interviennent. Le groupe D_{v_n} est alors associé à une place v_n de K_n au dessus d'une place v de K qui n'est pas totalement décomposée dans K_∞/K. On a une injection de D_{v_n} dans G_n, qui nous informe que le nombre minimal de générateurs de D_{v_n} est inférieur à d pour n assez grand. Le p-rang de $D^{ab}_{v_n}$ est donc inférieur à d. On en déduit que le p-rang de $\mathcal{D}_n$ est borné par d fois le cardinal de l'ensemble des places v_n que l'on considère. La place v n'étant pas totalement décomposée, le lemme qui suivant de voir que le nombre de places v_n au dessus de v évolue en $O(p^{n(d-1)})$.

Lemme 3.3 [Hachimori et Sharifi 2005, lemme 4.2]. *Soit v une place de K qui n'est pas totalement décomposée dans K_∞/K. On note V_n l'ensemble des places de K_n divisant v. Alors*

$$\#(V_n) = O(p^{n(d-1)}).$$

Démonstration. On fixe une place w de K_∞ au dessus de v. La place v n'étant pas totalement décomposée et G étant sans torsion, on en déduit que le sous-groupe de décomposition $G_v \subset G$, associé à $w|v$, est de dimension $d_v > 0$. On note $G_{v,n}$ la filtration de G_v induite par la filtration G_n de G. La proposition 1.3 nous informe que, pour n assez grand, il existe des constantes C et C' telles que

$$(G : G_n) = Cp^{nd} \quad \text{et} \quad (G_v : G_{v,n}) = C' p^{nd_v}.$$

Mais

$$\#(V_n) = (G/G_n : G_v/G_{v,n}) = \frac{C}{C'} p^{n(d-d_v)}. \qquad \square$$

Finalement, comme les places v à considérer sont en nombre fini, on obtient $\#(\mathscr{D}_n/p^n) = p^{O(np^{n(d-1)})}$ et

$$\#(\mathscr{G}_n^{ab}/p^n) = \#(X_n/p^n)p^{O(np^{n(d-1)})}.$$

La seconde équivalence se démontre en utilisant les mêmes arguments, le corollaire 2.3 remplaçant corollaire 2.4. La preuve de la dernière assertion est similaire, la suite exacte d'inflation-restriction étant à prendre à coefficients dans $\mathbb{Z}_p$. $\square$

On est alors en mesure de voir que le comportement asymptotique des p-groupes des classes $X_{S,n}^T$ est contrôlé par les invariants d'Iwasawa de l'extension. Le résultat suivant est le théorème 0.1 de l'introduction :

Corollaire 3.4. *Sous les hypothèses de cette section, on a les trois identités* :

$$\begin{aligned}
\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}^T) &= \rho_S^T (G : G_n) + O(p^{n(d-1)}),\\
\#(X_{S,n}^T/p^n) &= p^{(\rho_S^T n + \mu_S^T)(G:G_n) + O(np^{n(d-1)})},\\
\dim_{\mathbb{F}_p}(X_{S,n}^T/p) &= (\rho_S^T + r_S^T)(G : G_n) + O(p^{n(d-1)}).
\end{aligned}$$

Démonstration. La proposition 3.2 relie les quantités se rapportant à $X_{S,n}^T$ aux coïnvariants $(X_{S,\infty}^T)_{G_n}$. Les deux dernières assertions découlent alors du théorème 2.1. Pour la première assertion, il faut substituer au théorème 2.1 le théorème 1.10 de [Harris 2000], qui affirme que

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,\infty}^T)_{G_n} = \rho_S^T (G : G_n) + O(p^{n(d-1)}). \qquad \square$$

Les formules de réflexion. A l'imitation de ce qui est fait dans [Jaulent 2005], [Jaulent et Maire 2003] ou [Maire 2005], on va utiliser les théorèmes de réflexion de Gras [1998, 2003] pour obtenir des informations sur les invariants relatifs au couple (S, T) par rapport à ceux relatifs au couple (T, S), lorsque $S \cup T$ contient l'ensemble des places p-adiques de K. Ces informations traduisent une dualité entre la ramification et la décomposition. La théorie de Kummer joue un rôle central dans les formules de réflexion, c'est pourquoi la présence de racines de l'unité est nécessaire.

On introduit les notations suivantes :

Définition 3.5. On note Pl_p l'ensemble des places p-adiques de K et $\mathrm{Pl}_\infty^{\mathbb{R}}$ celui de ses places réelles.

Pour S un ensemble fini de places de K, on note S_0 l'ensemble des places finies de S, S_∞ l'ensemble de ses places infinies et S_p l'ensemble de ses places p-adiques.

- On note $s_\infty^{\mathbb{R}}$ le nombre de places réelles de S et s_0 le nombre de places finies de S. Si S ne contient que des places finies, on notera s à la place de s_0.
- On note s_0^{dec} le nombre de places de S_0 totalement décomposées dans K_∞/K. On le notera aussi s^{dec} si S ne contient que des places finies.
- On pose $\delta_S = \sum_{v \in S_p} [K_v : \mathbb{Q}_p]$ le degré p-adique en S.

La formule de réflexion sur laquelle on se base dans un premier temps est la suivante :

Théorème 3.6 [Gras 2003, théorème I.4.6]. *Soit p un premier et K un corps de nombres contenant μ_p, de signature (r_1, r_2). On se donne S et T deux ensembles finis disjoints de places de K vérifiant $\mathrm{Pl}_p \cup \mathrm{Pl}_\infty^{\mathbb{R}} \subset S \cup T$. On a alors la formule suivante, concernant les groupes des classes généralisées associés à K :*

$$\dim_{\mathbb{F}_p}(X_S^T/p) - \dim_{\mathbb{F}_p}(X_T^S/p) = s_0 - t_0 + \delta_S - r_1 - r_2 + \delta_{2,p}\, s_\infty^{\mathbb{R}},$$

où $\delta_{2,p} = 1$ si $p = 2$ et 0 sinon.

Cas $p = 2$. On commence par traiter le cas $p = 2$. On remarque tout d'abord que les places à l'infini n'ont aucune incidence sur l'invariant ρ.

Proposition 3.7.
$$\rho_S^T = \rho_{S_0}^{T_0}.$$

Démonstration. Il est clair que $X_{S,\infty}^T = X_{S_0,\infty}^{T \cup \mathrm{Pl}_\infty - S_\infty}$. La théorie du corps de classes donne alors une suite exacte

$$\bigoplus_{T_\infty \cup \mathrm{Pl}_\infty - S_\infty} \mathbb{Z}/2\mathbb{Z} \to X_{S_0,\infty}^{T_0} \to X_{S_0,\infty}^{T \cup \mathrm{Pl}_\infty - S_\infty} \to 0$$

qui conduit au résultat car le premier terme est de Λ-torsion. □

Les invariants d'Iwasawa de l'extension K_∞/K vérifient :

Théorème 3.8. *Pour $p=2$ et $\mathrm{Pl}_p \cup \mathrm{Pl}_\infty^{\mathbb{R}} \subset S \cup T$, on a*

$$\rho_S^T + r_S^T + \frac{\delta_T}{2} + t_0^{\mathrm{dec}} + \frac{t_\infty^{\mathbb{R}}}{2} = \rho_T^S + r_T^S + \frac{\delta_S}{2} + s_0^{\mathrm{dec}} + \frac{s_\infty^{\mathbb{R}}}{2}.$$

Démonstration. Le théorème 3.6 nous indique que pour tout n,

$$\begin{aligned}\dim_{\mathbb{F}_p}(X_{S,n}^T/p) &- \dim_{\mathbb{F}_p}(X_{T,n}^S/p) \\ &= s_0(K_n) - t_0(K_n) + \delta_S(K_n) - r_1(K_n) - r_2(K_n) + s_\infty^{\mathbb{R}}(K_n).\end{aligned}$$

Il faut remarquer ici que l'on a

$$\begin{aligned} r_1(K_n) + r_2(K_n) &= \tfrac{1}{2}(r_1(K_n) + 2r_1(K_n) + r_1(K_n)) \\ &= \tfrac{1}{2}\left(\delta_S(K_n) + \delta_T(K_n) + s_\infty^{\mathbb{R}}(K_n) + t_\infty^{\mathbb{R}}(K_n)\right).\end{aligned}$$

Le passage à la deuxième ligne se justifie grâce à l'hypothèse $\mathrm{Pl}_p \cup \mathrm{Pl}_\infty^{\mathbb{R}} \subset S \cup T$. La quantité $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$ est alors égale à

$$s_0(K_n) - t_0(K_n) + \frac{\delta_S(K_n)}{2} - \frac{\delta_T(K_n)}{2} + \frac{s_\infty^{\mathbb{R}}(K_n)}{2} - \frac{t_\infty^{\mathbb{R}}(K_n)}{2}.$$

Asymptotiquement, on a

$$\delta_S(K_n) = \delta_S(G:G_n) \quad \text{et} \quad s_0(K_n) = s_0^{\mathrm{dec}}(G:G_n) + O(p^{n(d-1)}),$$

car le lemme 3.3 permet de négliger les places qui ne sont pas totalement décomposées. Le groupe G est sans torsion donc les places de S_∞ sont totalement décomposées dans K_∞/K. On en déduit que $s_\infty^{\mathbb{R}}(K_n) = s_\infty^{\mathbb{R}}(G:G_n)$. Les mêmes considérations pour T conduisent à la formule

$$\begin{aligned}\dim_{\mathbb{F}_p}(X_{S,n}^T/p) &- \dim_{\mathbb{F}_p}(X_{T,n}^S/p) \\ &= \left(s_0^{\mathrm{dec}} - t_0^{\mathrm{dec}} + \frac{\delta_S}{2} - \frac{\delta_T}{2} + \frac{s_\infty^{\mathbb{R}}}{2} - \frac{t_\infty^{\mathbb{R}}}{2}\right)(G:G_n) + O(p^{n(d-1)}).\end{aligned}$$

On obtient la formule de l'énoncé en comparant avec le comportement asymptotique de $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$ donné par le corollaire 3.4. □

Cas $p \neq 2$ et $\mu_p \subset K$. La complexification des places réelles ne produit que de la 2-torsion dans les p-groupes X_S^T. Comme p est différent de 2 dans cette section les places réelles ne jouent aucun rôle. On peut donc considérer ici que S et T contiennent uniquement des places finies.

Dans ce paragraphe, on fait l'hypothèse que μ_p, le groupe des racines p-ièmes de l'unité, est inclu dans K. Le corps K est alors totalement imaginaire et on obtient :

Théorème 3.9. *Lorsque $\mu_p \subset K$ avec p impair et sous l'hypothèse que* $\mathrm{Pl}_p \subset S \cup T$, *on a la formule suivante concernant les invariants ρ et r :*

$$\rho_S^T + r_S^T + \frac{\delta_T}{2} + t^{\mathrm{dec}} = \rho_T^S + r_T^S + \frac{\delta_S}{2} + s^{\mathrm{dec}}.$$

Démonstration. Sous ces hypothèses, le terme de droite de la formule du théorème 3.6 devient

$$s(K_n) - t(K_n) + \delta_S(K_n) - \tfrac{1}{2}[K_n : \mathbb{Q}].$$

La relation $[K_n : \mathbb{Q}] = \delta_S(K_n) + \delta_T(K_n)$, provenant de l'hypothèse $\mathrm{Pl}_p \subset S \cup T$, ainsi que le lemme 3.3, qui permet de négliger les places qui ne sont pas totalement décomposées, donnent alors l'évolution

$$\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p) = \Big(s^{\mathrm{dec}} - t^{\mathrm{dec}} + \frac{\delta_S}{2} - \frac{\delta_T}{2}\Big)(G : G_n) + O(p^{n(d-1)}).$$

On conclut en invoquant le corollaire 3.4, qui donne l'évolution asymptotique de $\dim_{\mathbb{F}_p}(X_{S,n}^T/p) - \dim_{\mathbb{F}_p}(X_{T,n}^S/p)$. □

Lorsque l'extension K_∞/K contient toutes les racines p-primaires de l'unité, les informations obtenues seront plus précises. On traite donc ce cas dans le paragraphe suivant.

Cas cyclotomique. On suppose toujours dans cette section que $\mu_p \subset K$ ($\mu_4 \subset K$ si $p = 2$), et également que K_∞/K contient la $\mathbb{Z}_p$-extension cyclotomique de K, soit $K(\mu_{p^\infty}) \subset K_\infty$.

Ces hypothèses assurent que, pour k assez grand, le corps K_{k+n} contient les racines p^n-ièmes de l'unité. En effet, G est produit semi-direct du groupe de Galois de la $\mathbb{Z}_p$-extension cyclotomique de K, noté Γ, par un sous-groupe distingué H de G. Prenons k assez grand pour que G_k soit p-saturé, de telle sorte que $G_{k+n} = G_k^{p^n}$. Pour tout n, les racines p^n-ièmes de l'unité sont fixées par H et par Γ^{p^n}, donc par $G_k^{p^n}$. Autrement dit, $\mu_{p^n} \subset K_{k+n}$. On fixe cette constante k dans la suite, en remarquant qu'elle est nulle dans le cas d'un groupe uniforme.

On aura besoin d'un certain nombre de notations qui servirons à énoncer le théorème fondamental de cette partie, qui exprime une lien entre le groupe des classes associé à la S-ramification, T-décomposition d'une part, et le radical kummerien associé à la T-ramification, S-décomposition d'autre part.

On pourra se référer à [Jaulent 1998] pour les notations de la théorie p-adique du corps de classes. La notation $\mathfrak{m}$ vaut pour un certain diviseur, construit sur les places de $S(K_{k+n})$. Le module $\mathcal{R}$ est le p-adifié des idéles principaux de K_{k+n} et $\mathcal{R}_{\mathfrak{m}}$ est son sous-module des idéles congrues à 1 modulo $\mathfrak{m}$. On appelle $\mathcal{E}_{\mathfrak{m}}^T$ le p-adifié des T-unités de K_{k+n} qui sont congrues à 1 modulo $\mathfrak{m}$. Comme expliqué dans [Jaulent et Maire 2003], le diviseur $\mathfrak{m}$ a été choisi de telle sorte que le quotient d'ordre p^n du p-groupe des T-classes de rayon $\mathfrak{m}$ de K_{k+n}, noté $\mathrm{Cl}_{\mathfrak{m}}^T$, soit isomorphe au quotient d'ordre p^n du groupe de Galois de sa pro-p-extension abélienne S-ramifiée T-décomposée maximale X_S^T, et que le radical kummérien du quotient de l'extension duale, T-ramifiée et S-décomposée, soit donné par $\mathrm{Rad}_{\mathfrak{m}}^T$. Enfin, $\mathfrak{R}_{\mathfrak{m}}^T[p^n]$ est un pseudo-radical qui permet de faire le lien entre les deux suites du théorème suivant et qui est défini par

$$\mathfrak{R}_{\mathfrak{m}}^T[p^n] = \left\{ p^n \otimes x \in p^{-n}\mathbb{Z}_p/\mathbb{Z}_p \otimes \mathcal{R}_{\mathfrak{m}} \mid x \in \mathcal{J}^T \mathcal{J}^{p^n} \right\},$$

où $\mathcal{J}$ est le p-groupe des idèles de K_{k+n} et $\mathcal{J}^T$ son sous-groupe des T-idèles.

Théorème 3.10 [Jaulent et Maire 2003, théorème 4]. *A chaque étage K_{k+n} de la tour K_∞/K, on a les suites exactes du miroir :*

$$\begin{tikzcd}
1 \arrow[r] & (\mathcal{R}/\mathcal{R}_{\mathfrak{m}})[p^n]/\mu_{p^n} \arrow[r] & \mathfrak{R}_{\mathfrak{m}}^T[p^n] \arrow[r] \arrow[d, equal] & \mathrm{Rad}_{\mathfrak{m}}^T[p^n] \arrow[r] & 1 \\
1 \arrow[r] & \mathcal{E}_{\mathfrak{m}}^T/p^n \arrow[r] & \mathfrak{R}_{\mathfrak{m}}^T[p^n] \arrow[r] & \mathrm{Cl}_{\mathfrak{m}}^T[p^n] \arrow[r] & 1
\end{tikzcd}$$

Le corollaire suivant résulte du calcul des cardinaux des termes des suites exactes du miroir, conjointement au corollaire 3.4. Il donne le théorème 0.2 annoncé en introduction.

Corollaire 3.11. *On suppose que $\mu_p \subset K$ et que K_∞ contient la $\mathbb{Z}_p$-extension cyclotomique de K. On a les formules suivantes, lorsque $\mathrm{Pl}_p \subset S \cup T$, concernant les invariants associés à l'extension K_∞/K :*

$$\rho_S^T + \frac{\delta_T}{2} = \rho_T^S + \frac{\delta_S}{2}, \quad r_S^T = r_T^S \quad \textit{et} \quad \mu_S^T = \mu_T^S.$$

Démonstration. Dans cette démonstration, les modules qui interviennent sont attachés au corps K_{k+n}.

• Tout d'abord, on fait apparaître les invariants d'Iwasawa en regardant les cardinaux des termes de droite des deux suites. En effet, $\mathrm{Cl}_{\mathfrak{m}}^T$ étant un groupe fini, on en déduit, d'après la théorie du corps de classes, que

$$\#(\mathrm{Cl}_{\mathfrak{m}}^T[p^n]) = \#(\mathrm{Cl}_{\mathfrak{m}}^T/p^n) = \#(\mathrm{Cl}_S^T/p^n) = \#(X_S^T/p^n).$$

D'autre part, utilisant la théorie de Kummer,

$$\#(\mathrm{Rad}_{\mathfrak{m}}^T[p^n]) = \#(\mathrm{Rad}_S^T[p^n]) = \#(\mathrm{Hom}(X_T^S/p^n, \mu_{p^n})) = \#(X_T^S/p^n).$$

Les arguments conduisant au corollaire 3.4 peuvent être modifiés pour tenir compte du décalage de k et conduisent à la formule :

$$\#(X_{S,k+n}^T/p^n) = p^{(\rho_S^T n + \mu_S^T)(G:G_{k+n}) + O(np^{n(d-1)})}.$$

Les invariants ρ_S^T, μ_S^T et ρ_T^S, μ_T^S interviennent donc dans les cardinaux de $\mathrm{Cl}_{\mathfrak{m}}^T[p^n]$ et de $\mathrm{Rad}_{\mathfrak{m}}^T[p^n]$ respectivement.

Il reste à calculer les cardinaux des termes de gauche. On s'appuie sur ce qui est fait dans [Jaulent et Maire 2003].

• Le lemme d'approximation nous permet de voir que $(\mathcal{R}/\mathcal{R}_{\mathfrak{m}})[p^n] \simeq \mathcal{U}^S/p^n$, où $\mathcal{U}^S$ désigne le produit sur les places de $S(K_{k+n})$ des complétés p-adiques des unités locales :

$$\mathcal{U}^S/p^n \simeq \prod_{v \in S_p(K_{k+n})} \mathbb{Z}/p^n\mathbb{Z}^{[K_{k+n,v}:\mathbb{Q}_p]} \prod_{v \in S(K_{k+n})} \mu_{p^n}.$$

La partie racines de l'unité contribue en $p^{O(np^{n(d-1)})}$. En effet, comme K_∞/K contient la $\mathbb{Z}_p$-extension cyclotomique, aucune place n'est totalement décomposée dans K_∞/K. On fait alors appel au lemme 3.3 pour conclure que $\#(S(K_{k+n})) = O(p^{n(d-1)})$.

Quant au produit restant, son cardinal est donné par $p^{\delta_S n(G:G_{k+n})}$. Le quotient par les racines globales de l'unité ne change rien (cardinal en $p^{O(n)}$) et on en déduit que

$$\#((\mathcal{R}/\mathcal{R}_{\mathfrak{m}})[p^n]/\mu_{p^n}) = p^{\delta_S n(G:G_{k+n})+O(np^{n(d-1)})}.$$

• Le dernier cardinal à calculer et celui de $\mathcal{E}_{\mathfrak{m}}^T/p^n$. On a $\#(\mathcal{E}_{\mathfrak{m}}^T/p^n) = \#(\mathcal{E}^T/p^n)p^{O(n)}$ car les $\mathbb{Z}_p$-modules $\mathcal{E}^T$ et $\mathcal{E}_{\mathfrak{m}}^T$ sont de même rang (pour vérifier cela on peut regarder l'injection $\mathcal{E}^T/\mathcal{E}_{\mathfrak{m}}^T \hookrightarrow \prod_{v|\mathfrak{m}} U_v/U_v^{\mathfrak{m}_v}$) et leur torsion est composée de racines globales de l'unité, dont le cardinal évolue en $p^{O(n)}$. On trouve le cardinal voulu en appliquant le théorème de Dirichlet sur les T-unités qui donne

$$\#(\mathcal{E}^T/p^n) = p^{\frac{1}{2}[K:\mathbb{Q}]\,n(G:G_{k+n})+O(np^{n(d-1)})}.$$

• Finalement, mettant ces calculs ensemble, on trouve les formules

$$\rho_S^T + \tfrac{1}{2}[K:\mathbb{Q}] = \rho_T^S + \delta_S \quad \text{et} \quad \mu_S^T = \mu_T^S.$$

La formule symétrique de l'énoncé concernant ρ provient alors de l'hypothèse $\mathrm{Pl}_p \subset S \cup T$, qui implique $[K:\mathbb{Q}] = \delta_S + \delta_T$.

• En recoupant avec les théorèmes 3.8 et 3.9, on obtient l'égalité entre r_S^T et r_T^S. □

On peut aussi déduire de ce résultat une formule de réflexion concernant le $\mathbb{Z}_p$-rang des modules $X_{S,n}^T$

Corollaire 3.12. *Sous les mêmes hypothèses, on a*

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{T,n}^S) - \mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}^T) = \Big(\frac{\delta_T}{2} - \frac{\delta_S}{2}\Big)(G:G_n) + O(p^{n(d-1)}).$$

Démonstration. Le corollaire 3.11 donne un lien entre ρ_S^T et ρ_T^S. On sait, d'après le corollaire 3.4, que l'invariant ρ contrôle le $\mathbb{Z}_p$-rang de X_n, d'où le résultat. □

Calcul des invariants. Dans [Jaulent et Maire 2003], les formules de réflexion débouchent sur le calcul de l'invariant ρ_S^T dans le cas CM, ainsi que sur des inégalités concernant les invariants μ_S^T lorsque S et T varient. Nous allons exhiber des résultats de ce type dans le cadre non-commutatif.

On suppose dans cette section que $p \neq 2$ ou que K est totalement imaginaire. On fait aussi l'hypothèse que K_∞/K contient la $\mathbb{Z}_p$-extension cyclotomique, ce qui assure les deux propriétés essentielles suivantes :

- Aucune place finie de K n'est totalement décomposée dans K_∞/K.
- L'extension K_∞/K vérifie la condition de Leopoldt faible.

La condition de Leopoldt faible exprime que le groupe d'homologie

$$H_2(G_S(K_\infty), \mathbb{Z}_p)$$

est nul dès lors que S contient les places p-adiques, avec $G_S(K_\infty)$ qui désigne le groupe de Galois de la pro-p-extension S-ramifiée maximale de K_∞. Il est démontré dans [Nguyen-Quang-Do 1984] que cette condition est vérifiée en présence de la $\mathbb{Z}_p$-extension cyclotomique.

On va utiliser une formulation équivalente de cette condition, en terme de rang d'unités, que l'on peut trouver dans [Maire 2011, proposition 4.9]. On donne ici les grandes lignes de la démonstration. Pour un ensemble fini S de places de K contenant les places p-adiques et les places ramifiées dans K_∞/K, on note K_S la pro-p-extension maximale S-ramifiée de K et $G_S(K) = \mathrm{Gal}(K_S/K)$. Le corps K_∞ est alors inclu dans K_S et on note $X_S = \mathrm{Gal}(K_S/K_\infty)^{ab} = G_S(K_\infty)^{ab}$. La condition $H_2(G_S(K_\infty), \mathbb{Z}_p) = 0$ permet de relier le Λ-rang de X_S à la caractéristique d'Euler–Poincaré de $G_S(K)$ qui est connue. On en déduit ensuite une formule pour $\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n})$ grâce à la première formule du corollaire 3.4, que l'on relie au défaut de Leopoldt $\mathscr{E}_{S,n} = \ker(\mathscr{E}_n \to \mathscr{U}_n^S)$ via la théorie du corps de classes. On rappelle que $\mathscr{E}_n$ est le tensorisé par $\mathbb{Z}_p$ du groupe des unités globales de K_n et que $\mathscr{U}_n^S$ désigne le produit des p-adifiés des unités locales en toutes les S-places de K_n (voir les notations avant le théorème 3.10).

On en déduit l'expression suivante de la condition de Leopoldt faible,

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathscr{E}_{S,n}) = O(p^{n(d-1)}).$$

Cette condition est bien évidemment vérifiée si on admet la conjecture de Leopoldt pour les étages K_n.

Indépendance en T et en $S - S_p$. Dans le cas de la $\mathbb{Z}_p$-extension cyclotomique, les invariants ρ_S^T et μ_S^T ne dépendent que de S_p. L'argument, provenant de la théorie du corps de classes, est que les p-adifiés des sous-groupes de décomposition des places au-dessus de T et d'inertie des places de $S - S_p$ dans $X_{S,\infty}$ sont des $\mathbb{Z}_p$-modules de rang au plus 1. C'est toujours vrai dans le cas général mais les places à considérer sont alors en nombre infini ce qui empêche de conclure. Il faut alors redescendre à $X^T_{S,n}$ pour démontrer :

Théorème 3.13. $\rho^T_S = \rho_{S_p}$, $\mu^T_S = \mu_{S_p}$ *et* $r^T_S = r_{S_p}$.

Démonstration. Comme remarqué juste avant, les sous-groupes de décomposition et d'inertie des places de $T \cup S - S_p$ dans $X_{S,n}$ sont de p-rang au plus 1. Ces sous-groupes sont asymptotiquement au nombre de $O(p^{n(d-1)})$ car les places en question ne sont pas totalement décomposées dans K_∞/K (lemme 3.3). On peut conclure dans ce cas que

$$\#(X^T_{S,n}/p^n) = \#(X_{S_p,n}/p^n)\, p^{O(np^{n(d-1)})}$$

et que

$$\dim_{\mathbb{F}_p}(X^T_{S,n}/p) = \dim_{\mathbb{F}_p}(X_{S_p,n}/p) + O(p^{n(d-1)}).$$

Le corollaire 3.4 permet d'en déduire les égalités annoncées. □

Calcul de ρ^T_S. On calcule l'invariant ρ^T_S lorsque les corps K_n sont totalement réels ou CM pour tout n, toujours en présence de la $\mathbb{Z}_p$-extension cyclotomique.

Pour le cas CM, on note τ la conjugaison complexe et $\hat{S} = S \cap S^\tau$. On a :

Théorème 3.14. (i) *Si K_∞ est totalement réel, alors*

$$\rho^T_S = 0.$$

(ii) *Si K_n est CM pour tout n, alors*

$$\rho^T_S = \frac{\delta_{\hat{S}}}{2}.$$

Démonstration. Le théorème 3.13 permet de se limiter au calcul de ρ_S pour S un ensemble de places p-adique de K.

On obtient des informations sur ρ_S à l'aide de la formule

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}) = \rho_S(G : G_n) + O(p^{n(d-1)})$$

du corollaire 3.4. La théorie du corps de classes relie cette quantité à un problème de plongement d'unités grâce à la suite exacte

$$\mathscr{E}_n \to \mathscr{U}^S_n \to X_{S,n} \to X_n \to 0.$$

Les modules X_n sont les p-groupes des classes classiques donc sont de $\mathbb{Z}_p$-torsion. On en déduit

$$\mathrm{rk}_{\mathbb{Z}_p}(X_{S,n}) = \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathscr{E}_n \to \mathscr{U}^S_n)).$$

C'est ce dernier conoyau que l'on va calculer.

(i) On commence par traiter le cas totalement réel. On a

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S)) \leqslant \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^{\mathrm{Pl}_p})).$$

Asymptotiquement, le $\mathbb{Z}_p$-rang du noyau de cette dernière application évolue en $O(p^{n(d-1)})$ d'après la condition de Leopoldt. Comme les corps K_n sont totalement réels, $\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{E}_n) = [K : \mathbb{Q}](G : G_n) - 1$ d'après le théorème de Dirichlet et $\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{U}_n^{\mathrm{Pl}_p}) = [K : \mathbb{Q}](G : G_n)$. On en tire que le $\mathbb{Z}_p$-rang de ce dernier conoyau évolue en $O(p^{n(d-1)})$, donc que $\rho_S = 0$.

(ii) On suppose maintenant que K_n est CM pour tout n et on commence par traiter le cas où S est stable par τ.

La composante $\mathbb{Z}_p$-libre de l'image de $\mathcal{E}_n \to \mathcal{U}_n^S$ est contenue dans la partie $+$ des unités locales. On a ici

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{E}_n) = r_2(G : G_n) - 1 \quad \text{et} \quad \mathrm{rk}_{\mathbb{Z}_p}(\mathcal{U}_n^{\mathrm{Pl}_p})^+ = r_2(G : G_n).$$

La condition de Leopoldt permet de conclure que

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to (\mathcal{U}_n^S)^+)) &\leqslant \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to (\mathcal{U}_n^{\mathrm{Pl}_p})^+)) \\ &= O(p^{n(d-1)}). \end{aligned}$$

On a alors

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S)) &= \mathrm{rk}_{\mathbb{Z}_p}(\mathcal{U}_n^S)^- + O(p^{n(d-1)}) \\ &= \frac{\delta_S}{2}(G : G_n) + O(p^{n(d-1)}). \end{aligned}$$

Ainsi, $\rho_S = \delta_S/2$.

A partir de maintenant, on ne suppose plus que S est stable par τ. Pour une place v d'un corps CM, l'action de τ nous informe qu'une unité d'image triviale dans U_v est aussi d'image triviale dans U_{v^τ}. Notons $\check{S} = S \cup S^\tau$ de telle sorte que pour tout n,

$$\mathcal{E}_{S,n} = \ker(\mathcal{E}_n \to \mathcal{U}_n^S) \quad \text{et} \quad \mathcal{E}_{\check{S},n} = \ker(\mathcal{E}_n \to \mathcal{U}_n^{\check{S}})$$

sont égaux.

Le diagramme suivant permet de comparer $\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S)$ à $\mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^{\check{S}})$, qui est connu car $\check{S}$ est stable par τ :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{E}_{S,n} & \longrightarrow & \mathcal{E}_n & \longrightarrow & \mathcal{U}_n^S & \longrightarrow & \mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^S) & \longrightarrow & 0 \\ & & \| & & \| & & & & & & \\ 0 & \longrightarrow & \mathcal{E}_{\check{S},n} & \longrightarrow & \mathcal{E}_n & \longrightarrow & \mathcal{U}_n^{\check{S}} & \longrightarrow & \mathrm{coker}(\mathcal{E}_n \to \mathcal{U}_n^{\check{S}}) & \longrightarrow & 0. \end{array}$$

On a donc

$$\begin{aligned}\mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathscr{E}_n \to \mathscr{U}_n^S)) &= \mathrm{rk}_{\mathbb{Z}_p}(\mathscr{U}_n^S) - \mathrm{rk}_{\mathbb{Z}_p}(\mathscr{U}_n^{\check{S}}) + \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{coker}(\mathscr{E}_n \to \mathscr{U}_n^{\check{S}}))\\ &= \Big(\delta_S - \delta_{\check{S}} + \frac{\delta_{\check{S}}}{2}\Big)(G:G_n) + O(p^{n(d-1)})\\ &= \Big(\frac{\delta_{\hat{S}} - \delta_{\check{S}}}{2} + \frac{\delta_{\check{S}}}{2}\Big)(G:G_n) + O(p^{n(d-1)})\\ &= \frac{\delta_{\hat{S}}}{2}(G:G_n) + O(p^{n(d-1)}),\end{aligned}$$

d'où $\rho_S = \delta_{\hat{S}}/2$. □

Calcul de μ_S^T et r_S^T. Les calculs sur l'invariant μ contenus dans [Jaulent et Maire 2003] sont encore valables ici et peuvent être étendus à r. Nous les retraçons succinctement, les démonstrations étant identiques à celles dans le cas de la $\mathbb{Z}_p$-extension cyclotomique.

On se place dans le cadre cyclotomique, c'est-à-dire que l'on suppose que K contient les racines p-ièmes de l'unité (μ_4 si $p=2$) et que K_∞/K contient la $\mathbb{Z}_p$-extension cyclotomique. Cette condition est ici nécessaire pour obtenir des informations sur μ et r via les formules de réflexion.

Proposition 3.15. *Sous ces hypothèses, on a :*

(i) $$\mu_S^T = \mu_{S_p} = \mu_{\mathrm{Pl}_p - S_p} \quad \text{et} \quad r_S^T = r_{S_p} = r_{\mathrm{Pl}_p - S_p}.$$

(ii) *Si de plus K_n est CM pour tout n et S_p est stable par conjugaison complexe, alors*

$$\mu_S^T \leqslant \mu \quad \text{et} \quad r_S^T \leqslant r,$$

où μ et r sont les invariants correspondant au cas $S = T = \varnothing$.

Démonstration. (i) On utilise le théorème 3.13 et le corollaire 3.11 pour écrire :

$$\mu_S^T = \mu_{S_p} = \mu_{S_p}^{\mathrm{Pl}_p - S_p} = \mu_{\mathrm{Pl}_p - S_p}^{S_p} = \mu_{\mathrm{Pl}_p - S_p},$$

ainsi que les mêmes égalités pour r.

(ii) Les hypothèses permettent d'utiliser la preuve du théorème 13 de [Jaulent et Maire 2003] sans changement. □

Remerciements

Je remercie le rapporteur pour avoir pris le temps de lire et de commenter cet article, en particulier pour m'avoir signalé qu'un résultat de Howson donnait une preuve plus succincte de la première partie du théorème 2.1. Merci aussi à John Coates pour m'avoir suggéré d'étendre mes résultats sur les groupes uniformes aux groupes p-valués. J'exprime aussi ma gratitude envers mon directeur de thèse, Christian Maire, pour m'avoir fait découvrir un pan très intéressant des mathématiques, ainsi que pour son aide précieuse.

Bibliographie

[Balister et Howson 1997] P. N. Balister et S. Howson, "Note on Nakayama's lemma for compact Λ-modules", *Asian J. Math.* **1**:2 (1997), 224–229. MR 99f:16047 Zbl 0904.16019

[Brumer 1966] A. Brumer, "Pseudocompact algebras, profinite groups and class formations", *J. Algebra* **4** (1966), 442–470. MR 34 #2650 Zbl 0146.04702

[Coates et al. 2003] J. Coates, P. Schneider et R. Sujatha, "Modules over Iwasawa algebras", *J. Inst. Math. Jussieu* **2**:1 (2003), 73–108. MR 2004b:11152 Zbl 1061.11060

[Cuoco et Monsky 1981] A. A. Cuoco et P. Monsky, "Class numbers in $\mathbf{Z}_p^d$-extensions", *Math. Ann.* **255**:2 (1981), 235–258. MR 82h:12010 Zbl 0437.12003

[Dixon et al. 1999] J. D. Dixon, M. P. F. du Sautoy, A. Mann et D. Segal, *Analytic pro-p groups*, 2^e^ éd., Cambridge Studies in Adv. Math. **61**, Cambridge University Press, 1999. MR 2000m:20039 Zbl 0934.20001

[Gabriel 1962] P. Gabriel, "Des catégories abéliennes", *Bull. Soc. Math. France* **90** (1962), 323–448. MR 38 #1144 Zbl 0201.35602

[Gras 1998] G. Gras, "Théorèmes de réflexion", *J. Théor. Nombres Bordeaux* **10**:2 (1998), 399–499. MR 2002g:11154 Zbl 0949.11058

[Gras 2003] G. Gras, *Class field theory: From theory to practice*, Springer, Berlin, 2003. MR 2003j:11138 Zbl 1019.11032

[Hachimori et Sharifi 2005] Y. Hachimori et R. T. Sharifi, "On the failure of pseudo-nullity of Iwasawa modules", *J. Algebraic Geom.* **14**:3 (2005), 567–591. MR 2006a:11138 Zbl 1085.11054

[Harris 1979] M. Harris, "p-adic representations arising from descent on abelian varieties", *Compositio Math.* **39**:2 (1979), 177–245. MR 80j:14035 Zbl 0417.14034

[Harris 2000] M. Harris, "Correction to: "p-adic representations arising from descent on abelian varieties" [Compositio Math. **39** (1979), no. 2, 177–245; MR0546966 (80j:14035)]", *Compositio Math.* **121**:1 (2000), 105–108. MR 2001b:11050

[Howson 2002] S. Howson, "Euler characteristics as invariants of Iwasawa modules", *Proc. London Math. Soc.* (3) **85**:3 (2002), 634–658. MR 2004c:11202 Zbl 1036.11053

[Jannsen 1989] U. Jannsen, "Iwasawa modules up to isomorphism", pp. 171–207 dans *Algebraic number theory*, édité par J. Coates et al., Adv. Stud. Pure Math. **17**, Academic Press, Boston, MA, 1989. MR 93c:11095 Zbl 0732.11061

[Jaulent 1986] J.-F. Jaulent, *L'arithmétique des l-extensions*, thèse d'État, Université de Franche-Comté Faculté des Sciences, Besançon, 1986. MR 88j:11080 Zbl 0601.12002

[Jaulent 1998] J.-F. Jaulent, "Théorie l-adique globale du corps de classes", *J. Théor. Nombres Bordeaux* **10**:2 (1998), 355–397. MR 2002c:11152 Zbl 0938.11052

[Jaulent 2005] J.-F. Jaulent, "Généralisation d'un théorème d'Iwasawa", *J. Théor. Nombres Bordeaux* **17**:2 (2005), 527–553. MR 2007e:11132 Zbl 1176.11052

[Jaulent et Maire 2003] J.-F. Jaulent et C. Maire, "Sur les invariants d'Iwasawa des tours cyclotomiques", *Canad. Math. Bull.* **46**:2 (2003), 178–190. MR 2004f:11118 Zbl 1155.11353

[Lazard 1965] M. Lazard, "Groupes analytiques p-adiques", *Inst. Hautes Études Sci. Publ. Math.* **26** (1965), 389–603. MR 35 #188 Zbl 0139.02302

[Lesieur et Croisot 1959] L. Lesieur et R. Croisot, "Sur les anneaux premiers noethériens à gauche", *Ann. Sci. École Norm. Sup.* (3) **76** (1959), 161–183. MR 22 #54 Zbl 0092.03802

[Maire 2005] C. Maire, "Sur la dimension cohomologique des pro-p-extensions des corps de nombres", *J. Théor. Nombres Bordeaux* **17**:2 (2005), 575–606. MR 2007b:11179

[Maire 2011] C. Maire, "Plongements locaux et extensions de corps de nombres", *Int. J. Number Theory* **7**:3 (2011), 721–738. MR 2805577 Zbl 05913797

[Nguyen-Quang-Do 1984] T. Nguyen-Quang-Do, "Formations de classes et modules d'Iwasawa", pp. 167–185 dans *Number theory* (Noordwijkerhout, 1983), édité par H. Jager, Lecture Notes in Math. **1068**, Springer, Berlin, 1984. MR 85j:11156

[Ribes et Zalesskii 2000] L. Ribes et P. Zalesskii, *Profinite groups*, Ergebnisse der Mathematik (3) **40**, Springer, Berlin, 2000. MR 2001k:20060 Zbl 0949.20017

[Serre 1966] J.-P. Serre, "Classes des corps cyclotomiques (d'après K. Iwasawa)", Exp. No. 174 dans *Séminaire Bourbaki,* 1958/1959, W. A. Benjamin, Amsterdam, 1966. Reimpression: pp. 83–93 dans *Séminaire Bourbaki* **5**, Soc. Math. France, Paris, 1995. MR 0197243

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Venjakob 2002] O. Venjakob, "On the structure theory of the Iwasawa algebra of a p-adic Lie group", *J. Eur. Math. Soc.* (*JEMS*) **4**:3 (2002), 271–311. MR 2004h:16029 Zbl 1049.16016

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2^{e} éd., Graduate Texts in Mathematics **83**, Springer, New York, 1997. MR 97h:11130 Zbl 0966.11047

Communicated by John H. Coates
Received 2010-07-19 Revised 2011-02-25 Accepted 2011-05-08

guillaume.perbet@univ-fcomte.fr *Laboratoire de Mathématiques, UMR 6623, UFR Sciences et Techniques, 16 route de Gray, 25030 Besançon, France*

Algebra & Number Theory

msp.berkeley.edu/ant

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2011 is US $150/year for the electronic version, and $210/year (+$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
http://msp.org/
A NON-PROFIT CORPORATION
Typeset in LaTeX

Algebra & Number Theory

Volume 5 No. 6 2011