Composantes isotypiques de pro-p-extensions de corps de nombres et p-rationalité

Christian Maire, Marine Rougnant

Publ. Math. Debrecen
Manuscript (August 23, 2018)

Composantes isotypiques de pro-p-extensions de corps de nombres et p-rationalité

By Christian Maire and Marine Rougnant

Abstract. Let p be a prime number, and let K/k be a finite Galois extension of number fields with Galois group Δ of order coprime to p. Let S be a finite set of non archimedean places of k including the set S_p of p-adic places, and let K_S be the maximal pro-p extension of K unramified outside S. Let $G := G_S/H$ be a quotient of $G_S := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$ on which Δ acts trivially. Put $\mathcal{X} := H/[H,H]$. In this paper, we study the φ-component $\mathcal{X}^\varphi$ of $\mathcal{X}$ for all $\mathbb{Q}_p$-irreductible characters φ of Δ, and, in particular, by assuming Leopoldt conjecture we show that for all non-trivial characters φ, the $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^\varphi$ is free if and only if the φ-component of the $\mathbb{Z}_p$-torsion of $G_S/[G_S,G_S]$ is trivial. We also make a numerical study of the freeness of $\mathcal{X}^\varphi$ in cyclic extensions K/$\mathbb{Q}$ of degree 3 and 4 (by using families of polynomials given by Balady, Lecacheux and more recently by Balady and Washington), but also in degree 6 dihedral extension over $\mathbb{Q}$: the results we get support a recent conjecture of Gras.

Introduction

Dans cet article, nous étudions la structure galoisienne de certaines pro-p-extensions de corps de nombres à ramification restreinte. Le cadre algébrique

Mathematics Subject Classification: 11R37, 11R29.
Key words and phrases: Extensions de corps de nombres à ramification restreinte, pro-p-groupes G_S, corps p-rationnels.
Ce travail a reçu le soutien de la Région Franche-Comté sur la période 2014/2017. Il a été finalisé à l'automne 2017, période au cours de laquelle le premier auteur était à l'Université Cornell dans le cadre du programme "Mobilité sortante" de la Région Bourgogne Franche-Comté. Les auteurs remercient Georges Gras de son intérêt pour ce travail ainsi que pour ses remarques constructives. Ils remercient également les rapporteurs pour leurs attentives lectures.

général est le suivant. Soit $\mathcal{G}$ un pro-p-groupe de type fini et soit $\mathcal{H}$ un sous-groupe fermé normal de $\mathcal{G}$. Posons $G := \mathcal{G}/\mathcal{H}$ puis $\mathcal{X} := \mathcal{H}/[\mathcal{H},\mathcal{H}]$, le quotient abélien maximal de $\mathcal{H}$. Dans [20] le premier auteur étudie la liberté du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}$ suivant les contextes arithmétiques (et la structure du groupe G). Dans ce présent article, nous étendons ce travail au cas où les objets en jeu sont munis d'une action semi-simple.

Typiquement, soit p un nombre premier et soit K/k une extension galoisienne finie de groupe de Galois Δ d'ordre étranger à p. Soit S un ensemble fini de places finies de k contenant l'ensemble des places p-adiques S_p. Notons par K_S la pro-p-extension maximale de K non-ramifiée en dehors de S et posons $\mathcal{G} = G_{\mathrm{K},S} := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$ (lorsque $p = 2$, nous supposons donc que les éventuelles places archimédiennes réelles de K restent réelles le long de K_S/K). Soit ensuite F/K une sous-extension de K_S/K obtenue par compositum avec le corps K d'une sous-extension galoisienne L/k de k_S/k. Posons $\mathcal{H} = \mathrm{Gal}(\mathrm{K}_S/\mathrm{F})$ puis $G := \mathcal{G}/\mathcal{H}$. Le groupe Δ agit semi-simplement sur $\mathcal{X} = \mathcal{H}/[\mathcal{H},\mathcal{H}]$. Notons alors par $\mathcal{X}^\varphi$ la φ-composante de $\mathcal{X}$, où ici φ désigne un caractère $\mathbb{Q}_p$-irréductible de Δ. Comme Δ et G commutent, $\mathcal{X}^\varphi$ peut être également muni d'une structure de $\mathbb{Z}_p[\![G]\!]$-module. Dans ce travail, nous regardons à quelle condition le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^\varphi$ est libre. Le résultat que nous obtenons montre que le caractère trivial $\varphi = \mathbb{1}$ joue un rôle bien particulier. En effet, l'obstruction obtenue à la liberté du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^{\mathbb{1}}$ dépend du corps F et du groupe G (retrouvant au passage le résultat principal de [20]). En revanche, en dehors de ce cas, nous prouvons entre autres le résultat suivant :

Théorème A. *Supposons la conjecture de Leopoldt vraie. Alors sous les notations précédentes, pour tout caractère φ non-trivial, le module $\mathcal{X}^\varphi$ est $\mathbb{Z}_p[\![G]\!]$-libre si et seulement si $\mathrm{Tor}_{\mathbb{Z}_p}\big(G_{\mathrm{K},S}^{ab}\big)^\varphi$ est trivial. De plus, quand $\mathcal{X}^\varphi \simeq \mathbb{Z}_p[\![G]\!]^{d_\varphi}$, on a $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}\big(G_{\mathrm{K},S}^{ab}\big)^\varphi$.*

Ici, $\mathrm{Tor}_{\mathbb{Z}_p}\big(G_{\mathrm{K},S}^{ab}\big)^\varphi$ désigne la φ-composante de la torsion du $\mathbb{Z}_p$-module $G_{\mathrm{K},S}^{ab} := G_{\mathrm{K},S}/[G_{\mathrm{K},S}, G_{\mathrm{K},S}]$. Remarquons que le résultat ne dépend pas du choix du sous-groupe $\mathcal{H}$ de $G_{\mathrm{K},S}$.

L'objet arithmétique essentiel est donc le $\mathbb{Z}_p$-module de torsion $\mathrm{Tor}_{\mathbb{Z}_p} G_{\mathrm{K},S}^{ab}$. Par un théorème de déploiement (voir [12, Chapitre III, §4, Théorème 4.1.5]), son étude se ramène au cas où $S = S_p$. Le groupe fini $\mathrm{Tor}_{\mathbb{Z}_p} G_{\mathrm{K},S_p}^{ab}$ est un profond objet arithmétique qui mesure l'obstruction au groupe G_{K,S_p} à être pro-p-libre (sous la conjecture de Leopoldt). Lorsque ce groupe est trivial on dit que le corps K est p-rationnel (toujours sous la conjecture de Leopoldt).

L'étude des corps p-rationnels a fait l'objet d'une grande quantité de travaux : citons par exemple Movaheddi-Nguyen [23], Gras-Jaulent [13], Jaulent-Nguyen [15], et plus récemment Greenberg [14], Gras [8], [9], mais aussi Pitoun-Varescon [27] et Barbulescu-Ray [3], au sujet notamment des heuristiques "à la Cohen-Lenstra" (p est fixé et K varie dans des familles d'extensions de signature donnée). On renvoie à [12, Chapitre IV, §3] pour une présentation détaillée de l'étude des corps p-rationnels.

Récemment, Gras a émis la conjecture suivante ([11, Conjecture 7.11]) :

Conjecture (Gras)**.** *Soit un corps de nombres* K. *Pour p assez grand, le corps* K *est p-rationnel.*

Ainsi, le théorème A associé à la conjecture de Gras indique que pour p assez grand le module $\mathcal{X}^{\varphi}$ est libre (pour tout caractère $\varphi \neq \mathbb{1}$ et quand $S = S_p$).

Le calcul de $\mathrm{Tor}_{\mathbb{Z}_p} G_{\mathrm{K},S_p}^{ab}$ fait intervenir deux quantités dont l'une devient triviale dès que le p-Sylow du groupe des classes $\mathrm{Cl}(\mathrm{K})$ de K est trivial. Lorsque c'est le cas, le module $\mathrm{Tor}_{\mathbb{Z}_p} G_{\mathrm{K},S_p}^{ab}$ s'identifie à la torsion du quotient des unités des complétés p-adiques par la fermeture des unités globales. La présence de racines p-èmes de l'unité dans un complété p-adique peut faire apparaître "trivialement" de la torsion dans ce dernier quotient. Ainsi, si on s'assure de plus qu'aucun complété p-adique ne contient de racine d'ordre p (ce qui est toujours le cas dès que $p > [\mathrm{K} : \mathbb{Q}]+1$), alors l'étude de $\mathrm{Tor}_{\mathbb{Z}_p} G_{\mathrm{K},S_p}^{ab}$ "se résume" à celle du *régulateur normalisé* défini par Gras [10, Définition 5.1]. Cette observation que l'on trouve déjà dans [12, Chapitre III, §4.14] montre que la liberté de $\mathcal{X}^{\varphi}$ est propice à une étude numérique : c'est ce que nous faisons également dans ce travail. Nous utilisons pour cela des familles de polynômes P données par Balady [1], Lecacheux [19] et Balady-Washington [2]. Le corps de décomposition $\mathrm{K}/\mathbb{Q}$ d'un tel P est cyclique de degré 3 ou 4 et son groupe des unités est engendré par les racines de P. À l'exception d'un nombre fini et bien déterminé de nombres premiers p, le test pour prouver la liberté de $\mathcal{X}^{\varphi}$ (en fait sa trivialité pour les situations étudiées ici) équivaut dans ce cas à vérifier qu'un certain polynôme à coefficients entiers n'est pas nul dans le quotient $\mathbb{Z}[X]/(P, p^2)$. Ce cadre rend les calculs simples et rapides : il n'est pas nécessaire de passer par le corps de nombres K et donc d'utiliser les fonctions du corps de classes de PARI/GP. Cela nous permet de tester, pour quelques corps de ces familles, la liberté de $\mathcal{X}^{\varphi}$ pour $p < 23 \times 10^7$ dans le cas cubique et pour $p < 15 \times 10^7$ dans le cas quartique. Nous développons également cette étude numérique dans une famille d'extensions diédrales de degré 6 (pour $p < 10^9$). Notons enfin que Pitoun-Varescon [27] et plus récemment Gras [9] ont donné des algorithmes qui déterminent $\mathrm{Tor}_{\mathbb{Z}_p} G_{\mathrm{K},S_p}^{ab}$ en toute généralité ; afin d'être

complet, nous utilisons ces programmes pour traiter le cas des nombres premiers mis de côté dès le départ.

Notre travail comporte trois sections.

Dans un premier temps, nous donnons les éléments algébriques essentiels pour notre étude. Nous nous appuyons en particulier sur le livre de Neukirch-Schmidt-Wingberg [25, Partie : Algebraic Theory] pour montrer que la suite exacte à sept termes issue de la suite spectrale de Hochschild-Serre est également une suite de Δ-modules. Nous passons alors en revue les applications immédiates de ce résultat clef, notamment quand $\mathcal{G}$ est pro-p-libre ou quand $\mathcal{G}$ est de Demushkin.

Nous développons ensuite quelques situations arithmétiques desquelles il ressort le théorème A et ses corollaires.

La troisième section est dédiée à l'étude numérique dans des familles d'extensions cubiques cycliques, des familles cycliques totalement réelles de degré 4 et des familles d'extensions diédrales de degré 6. Les tableaux présentant les résultats de cette étude sont dressés en Appendice. Nous observons alors de façon éclatante la rareté des nombres premiers pour lesquels $\mathcal{X}^{\varphi}$ n'est pas libre, confirmant ainsi la conjecture de Gras évoquée précédemment.

L'ensemble des calculs ont été effectués à l'aide du logiciel PARI/GP [26].

Notations

Soit p un nombre premier. Si M désigne un $\mathbb{Z}_p$-module de type fini, nous notons par

- $\mathrm{rg}_{\mathbb{Z}_p} M$ le $\mathbb{Z}_p$-rang de M, *i.e* la dimension sur $\mathbb{Q}_p$ de $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$;
- $\mathrm{Tor}_{\mathbb{Z}_p} M$, le sous-module de torsion de M ;
- $M[p] = \{x \in M,\ px = 0\}$, les éléments de p-torsion de M ;
- $d_p M$ le nombre minimal de générateurs de M, *i.e.* la dimension sur $\mathbb{F}_p$ de $\mathbb{F}_p \otimes_{\mathbb{Z}_p} M$.

Si de plus M est muni d'une action d'un groupe fini Δ, nous notons par

- M^{Δ} le sous-groupe des invariants de M sous l'action de Δ ;
- M_{Δ} les coinvariants de M sous l'action de Δ.

On étend ces deux dernières notations au cas où Δ est profini avec action continue de Δ.

1. Quelques précisions algébriques

Une bonne référence pour une partie des résultats présentés dans cette section est le livre de Neukirch, Schmidt et Wingberg [25, Partie "Algebraic Theory"].

1.1. Le contexte algébrique.

1.1.1. *Généralités.* Soient $\mathcal{G}$ un pro-p-groupe de type fini, $\mathcal{H}$ un sous-groupe fermé normal de $\mathcal{G}$ et le quotient $G := \mathcal{G}/\mathcal{H}$. Posons $\mathcal{X} := \mathcal{H}^{ab} = \mathcal{H}/[\mathcal{H},\mathcal{H}]$. Soit l'algèbre d'Iwasawa complète

$$\mathbb{Z}_p[\![G]\!] = \varprojlim_U \mathbb{Z}_p[G/U],$$

où la limite projective est prise sur les sous-groupes ouverts normaux U de G. Notons I_G l'idéal d'augmentation de $\mathbb{Z}_p[\![G]\!]$, c'est le noyau du morphisme d'augmentation :

$$I_G = \ker\left(\mathbb{Z}_p[\![G]\!] \twoheadrightarrow \mathbb{Z}_p\right).$$

L'algèbre $\mathbb{Z}_p[\![G]\!]$ est un anneau local d'idéal maximal $\mathfrak{M}_G := p\mathbb{Z}_p[\![G]\!] + I_G$ pour laquelle il vient $\mathbb{Z}_p[\![G]\!]/\mathfrak{M}_G \simeq \mathbb{F}_p$.

Lemme 1.1. *Le pro-p-groupe abélien $\mathcal{X}$ est naturellement muni d'une structure de $\mathbb{Z}_p[\![G]\!]$-module (d'action continue pour les topologies naturelles sous-jacentes issues des limites projectives).*

Par le lemme de Nakayama topologique (voir par exemple [25, Chapitre V, §2]), le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}$ est de type fini si et seulement si le $\mathbb{F}_p$-module $\mathcal{X}/\mathfrak{M}_G$ l'est.
L'étude de la suite exacte

$$1 \longrightarrow \mathcal{H} \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 1$$

apporte le lemme suivant :

Lemme 1.2. *Si l'on suppose finis les groupes de cohomologie $H^2(\mathcal{G},\mathbb{F}_p)$ et $H^1(\mathcal{G},\mathbb{F}_p)$, alors le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}$ est de type fini.*

Remarque 1.3. Dans nos contextes arithmétiques on aura $\mathcal{G} = G_{\mathrm{K},S}$, et ces groupes sont bien de présentations finies (voir par exemple [16, Chapter 11], [25, Chapter X, §7] ou encore [12, Annexe]).

1.1.2. *Action semi-simple.* Soit Δ un groupe fini d'ordre premier à p. L'algèbre $\mathbb{Z}_p[\Delta]$ est munie d'un système fondamental d'idempotents orthogonaux $(e_\varphi)_\varphi$, φ parcourant l'ensemble $\mathrm{Irr}(\Delta, \mathbb{Q}_p)$ des caractères $\mathbb{Q}_p$-irréductibles de Δ. Si φ désigne un caractère $\mathbb{Q}_p$-irréductible de Δ, nous notons par $M^\varphi := e_\varphi M$ la φ-composante de M. Soient $\mathbb{1}$ le caractère trivial puis $\mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p) = \mathrm{Irr}(\Delta, \mathbb{Q}_p)\backslash\{\mathbb{1}\}$, l'ensemble des $\mathbb{Q}_p$-caractères irréductibles et non-triviaux de Δ.
Notons que $M^\Delta = M^{\mathbb{1}}$; la décomposition de M suivant les caractères irréductibles nous indique que $M^\Delta = \{0\}$ si et seulement si $M_\Delta = \{0\}$. Pour plus de détails, voir par exemple [5].

À présent, on suppose que Δ est un sous-groupe du groupe des automorphismes (continus) d'un pro-p-groupe de type fini $\mathcal{G}$. Notons par $\mathcal{G}(\Delta)$ la clôture normale dans $\mathcal{G}$ du groupe engendré par les élements $g^{-1}\sigma(g), g \in \mathcal{G}$, $\sigma \in \Delta$, et posons $\mathcal{G}_\Delta := \mathcal{G}/\mathcal{G}(\Delta)$. Ainsi, $\mathcal{G}_\Delta$ est le plus grand quotient de $\mathcal{G}$ sur lequel Δ agit trivialement. Soit le produit semi-direct $\Gamma := \Delta \ltimes \mathcal{G}$ induit par l'action de Δ sur $\mathcal{G}$.

Proposition 1.4 (Wingberg)**.** *On a $\mathcal{G}_\Delta \simeq \Gamma(p)$, où $\Gamma(p)$ est le pro-p-quotient maximal de Γ. De plus, $H^1(\mathcal{G}_\Delta, \mathbb{F}_p) \simeq H^1(\mathcal{G})^\Delta$ et $H^2(\mathcal{G}_\Delta, \mathbb{F}_p) \hookrightarrow H^2(\mathcal{G}, \mathbb{F}_p)^\Delta$. En particulier $\mathcal{G}_\Delta$ est pro-p-libre dès que $H^2(\mathcal{G}, \mathbb{F}_p)^\Delta = \{0\}$.*

Démonstration. Voir [34, Lemme 2] (la preuve y est donnée quand Δ est d'ordre 2 mais elle reste valable dès que Δ est d'ordre premier à p). Voir également [32, Proposition 1.4]. □

Lorsque $\mathcal{G}$ est de Demushkin (pour un rappel sur les groupes de Demushkin voir par exemple [25, Chapitre III, §9]), on a même plus :

Proposition 1.5 (Wingberg)**.** *Supposons $\mathcal{G}$ de Demushkin de dimension cohomologique stricte 2. Alors $H^2(\mathcal{G}_\Delta, \mathbb{F}_p) \simeq H^2(\mathcal{G}, \mathbb{F}_p)^\Delta$. Si de plus $H^2(\mathcal{G}, \mathbb{F}_p)^\Delta$ n'est pas trivial, le quotient $\mathcal{G}_\Delta$ est également de Demushkin.*

Démonstration. Voir [32, proposition 2.2] (ici il est inutile de se restreindre à la condition où Δ est d'ordre 2). □

Pour toute la suite, on prend $\mathcal{H}$ un sous-groupe fermé normal de $\mathcal{G}$ contenant $\mathcal{G}(\Delta)$ pour la raison suivante : le groupe Δ agit trivialement sur le quotient $\mathcal{G}_\Delta \twoheadrightarrow \mathcal{G}/\mathcal{H} := G$. Ainsi comme G et Δ commutent, le $\mathbb{Z}_p$-module $\mathcal{X} = \mathcal{H}/[\mathcal{H}, \mathcal{H}]$ hérite d'une structure de $\mathbb{Z}_p[\![G]\!]$-module, de type fini si $\mathcal{X}$ l'est. Traitons le caractère trivial.

Proposition 1.6. *Pour $\mathcal{H} = \mathcal{G}(\Delta)$, il vient $\mathcal{X}^{\mathbb{1}} = \{0\}$.*

DÉMONSTRATION. En effet, supposons que $\mathcal{X}^{\mathbb{1}}$ n'est pas trivial. Alors il existe un sous-groupe normal $\mathcal{H}_0$ de $\mathcal{G}$, sous-groupe strict de $\mathcal{G}(\Delta)$, tel que Δ agisse trivialement sur le quotient $G' := \mathcal{G}(\Delta)/\mathcal{H}_0$ (on peut par exemple s'assurer que $|G'| = p$) : cela repose sur le fait que le pro-p-groupe $\mathcal{G}_\Delta$ agit sur le pro-p-groupe $\mathcal{X}^{\mathbb{1}}$. Posons $G = \mathcal{G}/\mathcal{H}_0$ et regardons l'action de Δ sur G. Soit $\sigma \in \Delta$ d'ordre $n \neq 1$, et soit $g \in G$. Alors $\sigma(g) = gh$ avec $h \in G'$. Or $\sigma(h) = h$. Ainsi $g = \sigma^n(g) = gh^n$ et par conséquent $h^n = 1$. Comme G' est un p-groupe, il vient que $h = 1$ et donc $\sigma(g) = g$. On vient ainsi de montrer que le groupe Δ agit trivialement sur un quotient de $\mathcal{G}$ contenant strictement $\mathcal{G}_\Delta$, ce qui contredit la maximalité de $\mathcal{G}_\Delta$. □

Terminons ce paragraphe par une première réduction possible quand $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$: par la proposition suivante, l'étude de la φ-composante $\mathcal{X}^\varphi$ pour un tel φ est réduite à la situation où $G = \mathcal{G}_\Delta$. Conservons le contexte de la section 1.1.2.

Proposition 1.7. *Soient $\mathcal{H}_1 \subset \mathcal{H}_2$ deux sous-groupes normaux fermés de $\mathcal{G}$ contenant $\mathcal{G}(\Delta)$. Pour $i = 1, 2$, soient les quotients $G_i = \mathcal{G}/\mathcal{H}_i$. Posons $\mathcal{X}_i = \mathcal{H}_i^{ab}$ puis $H := \mathcal{H}_2/\mathcal{H}_1$. Alors pour tout caractère $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$, il vient l'isomorphisme de $\mathbb{Z}_p[\![G_2]\!]$-module : $(\mathcal{X}_{1,H})^\varphi \simeq \mathcal{X}_2^\varphi$. En particulier, si $\mathcal{X}_1^\varphi$ est $\mathbb{Z}_p[\![G_1]\!]$-libre, il en est de même pour $\mathcal{X}_2^\varphi$ en tant que $\mathbb{Z}_p[\![G_2]\!]$-module.*

DÉMONSTRATION. On part de la suite exacte $1 \longrightarrow \mathcal{H}_1 \longrightarrow \mathcal{H}_2 \longrightarrow H \longrightarrow 1$ qui devient

$$\cdots \longrightarrow H_1(H, \mathbb{Z}_p) \longrightarrow \mathcal{X}_{1,H} \longrightarrow \mathcal{X}_2 \longrightarrow H^{ab} \longrightarrow 1.$$

Il suffit ensuite de prendre les φ-composantes et d'utiliser le fait que Δ agit trivialement sur le quotient H et donc aussi sur $H_1(H, \mathbb{Z}_p)$ et sur H^{ab}. □

1.2. Suite spectrale à sept termes. Le point de départ algébrique de notre étude est, comme dans [20], la suite exacte à sept termes issue de la suite spectrale de Hochschild-Serre que l'on peut trouver dans [25, Chapitre II, §2, exercice 5].

Proposition 1.8. *Soit $\mathcal{G}$ un pro-p-groupe de type fini et soit $\mathcal{H}$ un sous-groupe de $\mathcal{G}$, distingué et fermé. On note G le quotient de $\mathcal{G}$ par $\mathcal{H}$ et on suppose que le groupe de cohomologie $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial. Alors on a la suite exacte d'homologie :*

$$\begin{array}{l} H_3(G, \mathbb{Z}_p) \longrightarrow H_1(G, \mathcal{H}^{ab}) \longrightarrow H_2(\mathcal{G}, \mathbb{Z}_p) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \big\downarrow \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad H_2(G, \mathbb{Z}_p) \longrightarrow (\mathcal{X}^{ab})_G \longrightarrow \mathcal{G}^{ab} \twoheadrightarrow G^{ab} \end{array} \tag{1}$$

La nouveauté ici consiste à regarder la suite exacte (1) dans le contexte d'une action semi-simple de Δ, en supposant que $\mathcal{G}(\Delta) \subset \mathcal{H}$. Rappelons que l'on note le quotient $G := \mathcal{G}/\mathcal{H}$.

Proposition 1.9. *Conservons le contexte de la proposition 1.8 et supposons $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p)$ et $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)$ triviaux. Alors la suite exacte (1) est également une suite exacte de $\mathbb{Z}_p[\Delta]$-modules.*

Démonstration. Sous l'hypothèse $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) = \{0\}$ la suite exacte (1) se scinde en deux suites exactes :

$$H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \hookrightarrow H^1(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)^G \twoheadrightarrow H^2(G, \mathbb{Q}_p/\mathbb{Z}_p), \tag{2}$$

$$H^1(G, H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p)) \hookrightarrow H^3(G, \mathbb{Q}_p/\mathbb{Z}_p). \tag{3}$$

L'action de $\sigma \in \Delta$ commute avec les applications inflation et restriction, donc avec les deux premiers morphismes de la suite exacte (2). Il nous reste à prouver que l'action de σ commute aussi avec la transgression (ce qui montrera également que σ commute avec le morphisme de la suite exacte (3)). La fin de la preuve est inspirée de [25, Chapitre I, §6, exercice 3]. Soit A un $\mathcal{G}$-module (discret). On définit le $\mathcal{G}$-module A_1 par la suite exacte

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}_{\mathcal{G}}(A) \longrightarrow A_1 \longrightarrow 0\ ,$$

où $\mathrm{Ind}_{\mathcal{G}}(A)$ est le module induit de A. On a alors la suite exacte longue de cohomologie

$$0 \longrightarrow A^{\mathcal{H}} \longrightarrow \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}} \longrightarrow A_1^{\mathcal{H}} \longrightarrow H^1(\mathcal{H}, A) \longrightarrow H^1(\mathcal{H}, \mathrm{Ind}_{\mathcal{G}}(A)) = \{0\}$$

que l'on coupe en deux en notant B l'image de $\mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}}$ dans $A_1^{\mathcal{H}}$:

$$0 \longrightarrow A^{\mathcal{H}} \longrightarrow \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}} \longrightarrow B \longrightarrow 0\ , \tag{4}$$

$$0 \longrightarrow B \longrightarrow A_1^{\mathcal{H}} \longrightarrow H^1(\mathcal{H}, A) \longrightarrow 0\ . \tag{5}$$

Soit maintenant $n \geqslant 1$. La suite exacte (4) donne

$$H^n(\mathcal{G}, \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}}) \longrightarrow H^n(\mathcal{G}, B) \longrightarrow H^{n+1}(\mathcal{G}, A^{\mathcal{H}}) \longrightarrow H^{n+1}(\mathcal{G}, \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}})\ ,$$

où les termes $H^n(\mathcal{G}, \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}})$ et $H^{n+1}(\mathcal{G}, \mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}})$ sont triviaux puisque $\mathrm{Ind}_{\mathcal{G}}(A)^{\mathcal{H}}$ est un $\mathcal{G}$-module induit. Finalement le δ-morphisme de connexion

$$\delta' : \ H^n(\mathcal{G}, B) \longrightarrow H^{n+1}(\mathcal{G}, A^{\mathcal{H}})$$

est un isomorphisme. Sa composée avec le δ-morphisme

$$\delta'' : \ H^{n-1}(\mathcal{G}, H^1(\mathcal{H}, A)) \longrightarrow H^n(\mathcal{G}, B)$$

obtenu à partir de la suite exacte (5) est, d'après [25, Chapitre II, §1, exercice 3], le morphisme $d_2^{n-1,1}$ associé à la suite spectrale de Hochschild-Serre. Comme l'action de σ commute avec les δ-morphismes de connexion, elle commute avec les morphismes $d_2^{n-1,1}$ et donc en particulier avec la transgression. □

1.3. Liberté des φ-composantes.

1.3.1. *Résultat préparatoire.* Soit G un pro-p-groupe de type fini et soit Δ un groupe fini d'ordre premier à p. On se donne un $\mathbb{Z}_p[\![G]\!][\Delta]$-module $\mathcal{Y}$ de type fini sur lequel les actions de G et Δ commutent.

Proposition 1.10. *Pour tout caractère irréductible φ de Δ, on a l'isomorphisme de Δ-modules : $H_1(G, \mathcal{Y}^{\varphi}) \simeq H_1(G, \mathcal{Y})^{\varphi}$.*

Démonstration. Commençons par le lemme suivant :

Lemme 1.11. *Sous les conditions précédentes, on a l'isomorphisme de Δ-modules : $(\mathcal{Y}_G)^{\varphi} \simeq (\mathcal{Y}^{\varphi})_G$. On notera par $\mathcal{Y}_G^{\varphi}$ ce Δ-module.*

Démonstration. Cela repose sur le fait que les actions de G et de Δ commutent. □

Soit une présentation minimale du $\mathbb{Z}_p[\![G \times \Delta]\!]$-module $\mathcal{Y}$:

$$1 \longrightarrow R \longrightarrow F \longrightarrow \mathcal{Y} \longrightarrow 1, \tag{6}$$

où $F \simeq \mathbb{Z}_p[\![G \times \Delta]\!]^r$. Pour φ un caractère irréductible de Δ, on projette la présentation de $\mathcal{Y}$ sur les φ-composantes pour obtenir :

$$1 \longrightarrow R^{\varphi} \longrightarrow F^{\varphi} \longrightarrow \mathcal{Y}^{\varphi} \longrightarrow 1 \ , \tag{7}$$

où ici F^{φ} est $\mathbb{Z}_p[\![G]\!]$-libre. La suite exacte (7) donne la suite exacte longue d'homologie :

$$1 \longrightarrow H_1(G, \mathcal{Y}^{\varphi}) \longrightarrow \underbrace{H_0(G, R^{\varphi})}_{(R^{\varphi})_G} \longrightarrow \underbrace{H_0(G, F^{\varphi})}_{(F^{\varphi})_G} \longrightarrow \underbrace{H_0(G, \mathcal{Y}^{\varphi})}_{(\mathcal{Y}^{\varphi})_G} \longrightarrow 1. \tag{8}$$

D'autre part, la G-homologie de (6) et les projections sur les φ-composantes donnent :

$$1 \longrightarrow H_1(G,\mathcal{Y})^\varphi \longrightarrow \underbrace{H_0(G,R)^\varphi}_{(R_G)^\varphi} \longrightarrow \underbrace{H_0(G,F)^\varphi}_{(F_G)^\varphi} \longrightarrow \underbrace{H_0(G,\mathcal{Y})^\varphi}_{(\mathcal{Y}_G)^\varphi} \longrightarrow 1. \quad (9)$$

Le résultat se déduit des suites exactes (8) et (9) associées au lemme 1.11. □

Corollaire 1.12. *Pour $\varphi \in \mathrm{Irr}(\Delta,\mathbb{Q}_p)$, le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{Y}^\varphi$ est libre si et seulement si les deux conditions suivantes sont satisfaites :*

(i) *$H_1(G,\mathcal{Y})^\varphi$ est trivial ;*

(ii) *$\mathcal{Y}_G^\varphi$ est $\mathbb{Z}_p$-libre.*

Démonstration. Il est bien connu qu'un $\mathbb{Z}_p[\![G]\!]$-module M de type fini est libre si et seulement si $H_1(G,M)$ est trivial et M_G est sans p-torsion. Il suffit alors simplement d'utiliser la proposition 1.10. □

1.3.2. *Un premier résultat et quelques conséquences.* Revenons au contexte de la section 1.1.2 et donnons une extension du résultat de [20] (voir aussi [25, Chapitre V, §6]) :

Théorème 1.13. *Soit $\mathcal{G}$ un pro-p-groupe de présentation finie et soit Δ un sous-groupe fini d'ordre premier à p du groupe des automorphismes de $\mathcal{G}$. Soit $\mathcal{H}$ un sous-groupe fermé normal de $\mathcal{G}$ contenant $\mathcal{G}(\Delta)$; posons $\mathcal{X} = \mathcal{H}/[\mathcal{H},\mathcal{H}]$ et $G = \mathcal{G}/\mathcal{H}$.*
Supposons $H_2(\mathcal{H},\mathbb{Z}_p)$ et $H_2(\mathcal{G},\mathbb{Z}_p)$ triviaux et fixons un caractère $\mathbb{Q}_p$-irréductible φ de Δ.

(i) *Pour $\varphi \neq \mathbb{1}$, le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^\varphi$ est libre si et seulement si le groupe $(\mathcal{G}^{ab})^\varphi$ est sans $\mathbb{Z}_p$-torsion et, dans ce cas, $\mathcal{X}^\varphi$ est de $\mathbb{Z}_p[\![G]\!]$-rang $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^\varphi$.*

(ii) *Pour $\varphi = \mathbb{1}$, supposons de plus G de dimension cohomologique $cd(G)$ au plus 2. Alors $\mathcal{X}^{\mathbb{1}}$ est $\mathbb{Z}_p[\![G]\!]$-libre dès que le morphisme $\mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\mathbb{1}} \to G^{ab}$ est injectif, et, dans ce cas, $\mathcal{X}^{\mathbb{1}}$ est de $\mathbb{Z}_p[\![G]\!]$-rang*

$$d_{\mathbb{1}} = d_p H_2(G,\mathbb{F}_p) - d_p G + \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\mathbb{1}}.$$

Remarque 1.14. Lorsque $\mathcal{Y} \simeq \mathbb{Z}_p[\![G]\!]^t$, l'entier t est unique. On l'appelle le $\mathbb{Z}_p[\![G]\!]$-rang de $\mathcal{Y}$.

Démonstration. Supposons $\varphi \neq \mathbb{1}$. Par hypothèse, le groupe Δ agit trivialement sur G et ainsi les φ-composantes $H_3(G,\mathbb{Z}_p)^\varphi$, $H_2(G,\mathbb{Z}_p)^\varphi$ et $(G^{ab})^\varphi$ sont triviales. La suite exacte de la proposition 1.8 implique alors

$$H_1(G,\mathcal{X})^\varphi = \{0\} \quad \text{et} \quad \mathcal{X}_G^\varphi \simeq (\mathcal{G}^{ab})^\varphi,$$

et on conclut grâce au corollaire 1.12.

Le cas du caractère trivial se traite de la même façon. Sous l'hypothèse $cd(G) \leqslant 2$, le groupe $H_3(G,\mathbb{Z}_p)^{\mathbb{1}}$ est trivial et il en est de même du groupe $H_1(G,\mathcal{X})^{\mathbb{1}}$. La suite exacte de la proposition 1.8 devient :

$$0 \longrightarrow H_2(G,\mathbb{Z}_p) \longrightarrow \mathcal{X}_G^{\mathbb{1}} \longrightarrow (\mathcal{G}^{ab})^{\mathbb{1}} \longrightarrow (G^{ab})^{\mathbb{1}} \longrightarrow 0$$

dont on déduit que le $\mathbb{Z}_p$-module $\mathcal{X}_G^{\mathbb{1}}$ est sans torsion si et seulement si le morphisme $\mathrm{Tor}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\mathbb{1}} \to (G^{ab})^{\mathbb{1}}$ est injectif (car $H_2(G,\mathbb{Z}_p)$ est sans torsion), et on peut conclure grâce au corollaire 1.12. Les calculs sur les rangs sont ensuite immédiats. □

Remarque 1.15. Notre résultat principal peut être vu comme une réciproque à la proposition 1.7. En effet, pour $\varphi \neq \mathbb{1}$, nous montrons que $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![G]\!]$-libre pour tout quotient G de $\mathcal{G}_\Delta$ si et seulement si $\mathcal{X}_0^{\varphi}$ est $\mathbb{Z}_p$-libre où $\mathcal{X}_0 := \mathcal{G}^{ab}$, en d'autres termes pour le plus petit quotient de $\mathcal{G}_\Delta$.

Remarque 1.16. Sous les conditions du théorème 1.13 et pour $\mathcal{H} = \mathcal{G}(\Delta)$, on obtient que $H^2(\mathcal{G}_\Delta, \mathbb{Q}_p/\mathbb{Z}_p)$ est trivial : en effet, dans ce cas, $\mathcal{X}^{\mathbb{1}} = \{0\}$.

Donnons à présent quelques situations immédiates (dans le contexte de la section 1.1.2).

Corollaire 1.17. *Soit $\mathcal{G}$ un pro-p-groupe de dimension cohomologique stricte 2 et soit $\mathcal{H}$ un sous-groupe fermé et distingué de $\mathcal{G}$ contenant $\mathcal{G}(\Delta)$. Soit $\mathcal{G}_0$ un sous-groupe ouvert et distingué de $\mathcal{G}$ contenant $\mathcal{H}$. Posons $G = \mathcal{G}/\mathcal{H}$ et $G_0 = \mathcal{G}_0/\mathcal{H}$. Alors pour $\varphi \in \mathrm{Irr}^{\bullet}(\Delta,\mathbb{Q}_p)$, le $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^{\varphi}$ est libre si et seulement si il l'est en tant que $\mathbb{Z}_p[\![G_0]\!]$-module.*

Démonstration. Un sens est immédiat, mais nous allons montrer ce résultat par équivalence directe. Comme $\mathcal{G}$ est de dimension cohomologique stricte 2, les hypothèses du théorème 1.13 sont satisfaites et ainsi $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![G]\!]$-libre si et seulement si $\mathrm{Tor}_{\mathbb{Z}_p}\left(\mathcal{G}^{ab}\right)^{\varphi}$ est trivial. Il en est de même de $\mathcal{X}^{\varphi}$ en tant que $\mathbb{Z}_p[\![G_0]\!]$-module. Mais l'hypothèse sur la dimension cohomologique stricte assure également un isomorphisme entre $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}^{ab}$ et $\left(\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}_0^{ab}\right)^{\mathcal{G}/\mathcal{G}_0}$ induit par le morphisme de transfert (voir par exemple [25, Chapitre III, Théorème 3.6.4]). Ainsi, les φ-composantes de $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}^{ab}$ et de $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}_0^{ab}$ sont simultanément nulles ou non. Le résultat s'en déduit. □

Corollaire 1.18. *Soit $\mathcal{G}$ un pro-p-groupe libre à d générateurs. Soit $\mathcal{H}$ un sous-groupe fermé et distingué de $\mathcal{G}$ contenant $\mathcal{G}(\Delta)$. Alors pour $\varphi \in \mathrm{Irr}^{\bullet}(\Delta,\mathbb{Q}_p)$, on a $\mathcal{X}^{\varphi} \simeq \mathbb{Z}_p[\![G]\!]^{d_\varphi}$, où $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\varphi}$.*

Démonstration. Immédiat. □

À ce niveau, on peut avancer un résultat un peu plus précis lorsque $\mathcal{H} = \mathcal{G}(\Delta)$. Rappelons que si F_d est le pro-p-groupe libre à d générateurs, l'algèbre $\mathbb{Z}_p[\![\mathrm{F}_d]\!]$ est isomorphe à l'algèbre de Magnus des séries formelles non commutatives $\mathbb{Z}_p[\![X_1, \cdots, X_d]\!]^{nc}$ (voir par exemple [16, Chapitre 7, §7.6]).

Corollaire 1.19. *Sous les conditions du théorème 1.13, prenons $\mathcal{H} = \mathcal{G}(\Delta)$. Supposons $(\mathcal{G}^{ab})^{\varphi}$ et $(\mathcal{G}^{ab})^{\mathbb{1}}$ sans $\mathbb{Z}_p$-torsion, où $\varphi \in \mathrm{Irr}^{\bullet}(\Delta, \mathbb{Q}_p)$. Alors*

$$\mathcal{X}^{\varphi} \simeq \left(\mathbb{Z}_p[\![X_1, \cdots, X_{d_1}]\!]^{nc}\right)^{d_{\varphi}},$$

où $d_{\varphi} = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\varphi}$.

Démonstration. Le théorème 1.13 indique ici que $\mathcal{X}^{\varphi}$ est libre de rang d_{φ}. De plus, la suite exacte $1 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{F}_p \longrightarrow 1$ apporte la suite exacte de Δ-modules

$$\cdots \longrightarrow H_2(\mathcal{G}, \mathbb{Z}_p) \longrightarrow H_2(\mathcal{G}, \mathbb{F}_p) \longrightarrow \mathcal{G}^{ab}[p].$$

Par hypothèse $H_2(\mathcal{G}, \mathbb{Z}_p) = \{0\}$ et $\left(\mathcal{G}^{ab}[p]\right)^{\mathbb{1}} = \{1\}$. Ainsi, $H_2(\mathcal{G}, \mathbb{F}_p)^{\mathbb{1}} = \{0\}$ et la proposition 1.4 indique que $\mathcal{G}_{\Delta}$ est pro-p-libre de rang égal au p-rang de $(\mathcal{G}^{ab})^{\mathbb{1}}$, c'est-à-dire à $\mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^{\mathbb{1}}$. □

Pour le dernier corollaire de cette section, faisons le rappel suivant : un groupe de Demushkin $\mathcal{G}$ est de dimension cohomologique stricte 2 si et seulement si pour tout sous-groupe ouvert $\mathcal{U}$ de $\mathcal{G}$, $H^2(\mathcal{U}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, ou encore si et seulement si $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{U}^{ab} \neq \{0\}$. La dernière équivalence provient de la suite exacte

$$1 \longrightarrow H_2(\mathcal{U}, \mathbb{Z}_p)/p \longrightarrow H_2(\mathcal{U}, \mathbb{F}_p) \longrightarrow \mathcal{U}^{ab}[p] \longrightarrow 1$$

associée au fait que $H_2(\mathcal{U}, \mathbb{F}_p) \simeq \mathbb{Z}/p\mathbb{Z}$ (pour la première équivalence voir par exemple [29, Chapitre I §3 Proposition 19]). Cette suite exacte indique également que si $\mathcal{G}$ est de dimension cohomologique stricte 2, on a l'isomorphisme de Δ-modules :

$$H_2(\mathcal{G}, \mathbb{F}_p) \simeq_{\Delta} \mathcal{G}^{ab}[p].$$

Corollaire 1.20. *Soit $\mathcal{G}$ un groupe de Demushkin de dimension cohomologique stricte 2. Soit ω le caractère de Δ résultant de l'action sur $\mathrm{Tor}_{\mathbb{Z}_p}\mathcal{G}^{ab}$.*

(i) *Si $\mathcal{G}_{\Delta}$ est pro-p-libre, alors $\mathcal{X}^{\omega}$ est non libre en tant que $\mathbb{Z}_p[\![\mathcal{G}_{\Delta}]\!]$-module et, pour $\varphi \neq \omega$, $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![\mathcal{G}_{\Delta}]\!]$-libre.*

(ii) *Si $\mathcal{G}_\Delta$ est de Demushkin, alors pour tout $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$, on a $\mathcal{X}^\varphi = \mathbb{Z}_p[\![\mathcal{G}_\Delta]\!]^{d_\varphi}$, avec $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^\varphi$.*

Démonstration. Comme $\mathcal{G}$ est de Demushkin de dimension cohomologique stricte 2, les conditions sur les multiplicateurs de Schur $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) = \{0\}$ et $H^2(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p) = \{0\}$ sont satisfaites pour tout sous-groupe fermé $\mathcal{H}$ de $\mathcal{G}$. Suivant la proposition 1.5, $\mathcal{G}_\Delta$ est pro-p-libre si et seulement si $H^2(\mathcal{G}, \mathbb{F}_p)^{\mathbb{1}} = \{0\}$. Dans ce cas $\omega \neq \mathbb{1}$ et $\mathcal{X}^\omega$ n'est pas libre. En revanche les autres φ-composantes sont libres. Dans l'autre cas, $H^2(\mathcal{G}, \mathbb{F}_p)^{\mathbb{1}}$ n'est pas trivial, ainsi $\omega = \mathbb{1}$ et $\mathcal{X}^\varphi$ est libre pour tout $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$. □

2. Études de quelques contextes arithmétiques

Si K désigne un corps de nombres ou un corps local et si p désigne un nombre premier, on note par $\mu_{p^\infty}(\mathrm{K})$ le groupe des racines de l'unité d'ordre une puissance de p contenues dans K.

2.1. La situation locale. Soit une extension locale K/k de $\mathbb{Q}_p$, galoisienne de groupe de Galois Δ, d'ordre premier à p. Notons par $\overline{\mathrm{K}}$ la pro-p-extension maximale de K et posons $\mathcal{G} = \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$. Soit $\Gamma = \Delta \ltimes \mathcal{G}$. Posons $\mathcal{H} = \mathcal{G}(\Delta)$, $\mathcal{X} = \mathcal{H}^{ab}$, $G = \mathcal{G}/\mathcal{G}_\Delta$. Le pro-$p$-groupe $G \simeq \mathcal{G}(p)$ est isomorphe au groupe de Galois $\mathrm{Gal}(\overline{\mathrm{k}}/\mathrm{k})$: c'est un pro-p-groupe à $[\mathrm{k} : \mathbb{Q}_p] + 1 + d_p\mu_{p^\infty}(\mathrm{K})$ générateurs. Suivant que k contient les racines p-èmes de l'unité ou non, le pro-p-groupe G est un groupe de Demushkin (de dimension cohomologique stricte 2) ou un pro-p-groupe libre.

Corollaire 2.1. *Supposons que* K *ne contient pas les racines p-èmes de l'unité. Alors pour tout caractère $\mathbb{Q}_p$-irréductible $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$, il vient $\mathcal{X}^\varphi \simeq \mathbb{Z}_p[\![G]\!]^{d_\varphi}$, avec $d_\varphi = \mathrm{rg}_{\mathbb{Z}_p}(\mathcal{G}^{ab})^\varphi = \deg(\varphi)[\mathrm{k} : \mathbb{Q}_p]$.*

Démonstration. Ici $\mathcal{G}$ est pro-p-libre, et c'est alors une application immédiate du corollaire 1.18. □

Supposons maintenant que K contient les racines p-èmes μ_p de l'unité. Alors $\mathcal{G}$ est un groupe de Demushkin et l'on se retrouve dans la situation du corollaire 1.20. Soit ω le caractère de Δ résultant de l'action sur μ_p.

Corollaire 2.2. *Supposons que* K *contient les racines p-èmes de l'unité.*

(i) *Pour $\varphi \neq \omega$ et $\varphi \neq \mathbb{1}$, il vient $\mathcal{X}^\varphi \simeq \mathbb{Z}_p[\![G]\!]^{d_\varphi}$, où $d_\varphi = \deg(\varphi)[\mathrm{k} : \mathbb{Q}_p]$.*

(ii) *Quand $\omega \neq \mathbb{1}$, $\mathcal{X}^\omega$ n'est pas $\mathbb{Z}_p[\![G]\!]$-libre.*

(iii) *Quand* $\omega = \mathbb{1}$, $\mathcal{X}^{\mathbb{1}} = \{0\}$.

DÉMONSTRATION. Seuls les caractères $\mathbb{1}$ et ω sont à discuter. Si ω n'est pas le caractère trivial, c'est le point (i) du corollaire 1.20 qui s'applique. Si $\omega = \mathbb{1}$, cela signifie que G est de Demushkin de dimension cohomologique stricte 2 et cette fois-ci, c'est le point (ii) qui s'applique. □

2.2. Extensions de corps de nombres.

2.2.1. *Rappels.* Le contexte que l'on va considérer par la suite est celui des extensions à ramification restreinte. Rappelons les points essentiels pour notre étude.

Soit p un nombre premier.

(*i*) Soit K un corps de nombres et soit S un ensemble fini de places finies de K contenant les places p-adiques. Notons par K_S la pro-p-extension maximale de K non-ramifiée en dehors de S, et posons $G_{\mathrm{K},S} = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$. Pour une place v de S, on note par $\mathcal{U}_v$ le p-Sylow du groupe des unités locales en v. Soit ensuite $\mathcal{E}_\mathrm{K} = \mathbb{Z}_p \otimes E_\mathrm{K}$ le p-adifié du groupe des unités E_K de K. L'ensemble S étant fixé, on note enfin par ι $(= \iota_S)$ le plongement diagonal de $\mathcal{E}_\mathrm{K}$ dans $\prod_{v\in S}\mathcal{U}_v$.

L'étude de $G_{\mathrm{K},S}^{ab} := (G_{\mathrm{K},S})^{ab}$ peut se faire de façon relative, par exemple à travers le p-groupe des classes $\mathrm{Cl}(\mathrm{K})$ de K (via l'application d'Artin). Typiquement (voir par exemple [12, Chapitre III]), on a :

Proposition 2.3. *Soit p tel que* $\mathrm{Cl}(\mathrm{K})$ *est trivial. Alors*

$$G_{\mathrm{K},S}^{ab} \simeq \frac{\prod_{v\in S}\mathcal{U}_v}{\iota(\mathcal{E}_\mathrm{K})}.$$

Cette proposition montre que les nombres premiers qui divisent l'ordre du groupe des classes jouent un rôle bien particulier pour notre étude. Nous les appelons *nombres premiers exceptionnels*. Rappelons que le théorème de Brauer-Siegel (cf [18, Chapitre XVI, §1]) apporte l'inégalité $|\mathrm{Cl}(\mathrm{K})| \leqslant |\mathrm{Disc}_\mathrm{K}|^C$, où Disc_K est le discriminant du corps K et où C est une constante universelle. Rappelons également qu'il est conjecturé que pour tout $\varepsilon > 0$: $|\mathrm{Cl}(\mathrm{K})[p]| \ll_{\varepsilon,[\mathrm{K}:\mathbb{Q}]} |\mathrm{Disc}_\mathrm{K}|^\varepsilon$. Voir par exemple Ellenberg-Venkatesh [7] pour une présentation de cette conjecture.

(*ii*) Soit K/k une extension galoisienne de corps de nombres de groupe de Galois Δ d'ordre premier à p. Pour S $(= S_\mathrm{k})$ un ensemble fini de places de k, nous notons également par S $(= S_\mathrm{K} = \{w|v, v \in S_\mathrm{k}, w \text{ place de K}\})$ l'ensemble des places de K au-dessus de celles de S_k. La proposition 2.3 fait apparaître le Δ-module $\prod_{w|v}\mathcal{U}_w$, et sa structure est bien connue. En effet, soit v une place de k et soit $w|v$ une place de K au-dessus de w. Par abus, posons $D_v = D_w$ le groupe décomposition de w

dans K/k. Si v ne divise pas p, le Δ-module $\prod_{w|v}\mathcal{U}_w$ est isomorphe au module induit $\mathrm{Ind}_{D_v}^{\Delta}\mu_{p^\infty}(\mathrm{K}_w) := \mathbb{Z}_p[\Delta]\otimes_{D_v}\mu_{p^\infty}(\mathrm{K}_w)$. À noter que si k_v contient une racine primitive p-ème de l'unité, alors D_v agit trivialement sur $\mu_{p^\infty}(\mathrm{K}_w)$ et ainsi $\prod_{w|v}\mathcal{U}_w \simeq \mathbb{Z}_p[\Delta]\otimes_{D_v}\mathbb{Z}/N\mathbb{Z}$, où $N = |\mu_{p^\infty}(\mathrm{k}_v)|$. Lorsque v divise p, le logarithme p-adique permet d'obtenir $\prod_{w|v}\mathcal{U}_w \simeq \mathrm{Ind}_{D_v}^{\Delta}\mu_{p^\infty}(\mathrm{K}_w)\oplus(\mathbb{Z}_p[\Delta])^{[\mathrm{k}_v:\mathbb{Q}_p]}$.

(*iii*) La conjecture de Leopoldt pour le corps de nombres K et le nombre premier p stipule que l'application de semi-localisation induit un $\mathbb{Z}_p$-morphisme injectif de $\mathcal{E}_\mathrm{K}$ dans le produit $\prod_{v|p}\mathcal{U}_v$. (Voir [12, Chapitre III, §3] ou [25, Chapitre X, §3] pour plus de précisions.) Rappelons que la conjecture de Leopoldt équivaut à la trivialité du multiplicateur de Schur $H_2(G_{\mathrm{K},S},\mathbb{Z}_p)$ du pro-p-groupe $G_{\mathrm{K},S}$ dès que S contient l'ensemble S_p (voir [24], et [30] pour $p=2$). Comme le pro-p-groupe $G_{\mathrm{K},S}$ est de dimension cohomologique au plus 2 (pour $p=2$, voir [30]), la conjecture de Leopoldt le long de K_S/K équivaut au fait que le pro-p-groupe $G_{\mathrm{K},S}$ est de dimension cohomologique stricte au plus 2, pour tout ensemble fini S contenant S_p.

On suppose pour toute la suite que la conjecture de Leopoldt est vérifiée pour toutes les extensions finies de K. Ainsi pour tout sous-groupe fermé de $\mathcal{H}$ de $G_{\mathrm{K},S}$ le groupe $H_2(\mathcal{H},\mathbb{Z}_p)$ est trivial : les hypothèses du théorème 1.13 seront vérifiées dans les contextes globaux à venir.

Terminons ce point en rappelant un théorème de déploiement de la ramification ([12, Chapitre III, §4, Théorème 4.1.5]) :

Théorème 2.4. *Supposons la conjecture de Leopoldt vérifiée pour le corps de nombres* K *et le premier* p*. Alors il vient la suite exacte*

$$1 \longrightarrow \prod_{v\in S\setminus S_p}\mathcal{U}_v \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p}G_{\mathrm{K},S}^{ab} \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p}G_{S_p}^{ab} \longrightarrow 1.$$

(*iv*) On se place donc sous la conjecture de Leopoldt. À l'exception d'un nombre fini de nombres premiers p d'après la proposition 2.3, nous verrons que l'object central de notre étude est la torsion du quotient $\prod_{v\in S_p}\mathcal{U}_v/\iota(\mathcal{E}_\mathrm{K})$. Lorsqu'il est trivial, le corps K est dit p-rationnel. Si de plus $|\mu_{p^\infty}(\mathrm{k}_v)| = 1$ pour tout $v|p$, alors notre étude est ramenée à celle du module de torsion

$$\mathrm{Tor}_{\mathbb{Z}_p}\left(\log_p\prod_{v\in S_p}\mathcal{U}_v/\log_p\iota(\mathcal{E}_\mathrm{K})\right),$$

appelé *régulateur (p-adique) normalisé* de K ([10, Définition 5.1]).

2.2.2. *Quelques situations immédiates.* Soit K/k une extension galoisienne de corps de nombres de groupe de Galois Δ d'ordre premier à p. Soit S un ensemble fini de places finies de k. On va appliquer les résultats de la section 1 au groupe $\mathrm{Gal}(\mathrm{K}_S/\mathrm{k}) =: \Gamma = \Delta \ltimes \mathcal{G}$, où l'on a posé $\mathcal{G} := \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$.

On notera v une place de S_k et $w|v$ une place de S_K au-dessus de v. Pour qu'une place $w \in S$ puisse jouer un rôle, nous nous assurons que :

- ou bien w est une place p-adique ;
- ou bien, si $w \nmid p$, le corps local K_w contient une racine primitive d'ordre p.

Remarquons que pour $v|w$, avec $v \nmid p$, on peut avoir $|\mu_{p^\infty}(\mathrm{k}_v)| = 1$.

Soit $G := \mathcal{G}_\Delta$ le plus grand quotient de $\mathcal{G}$ sur lequel Δ agit trivialement. On a alors :

Lemme 2.5. *Le groupe de Galois G est isomorphe au groupe de Galois* $\mathrm{Gal}(\mathrm{k}_S/\mathrm{k})$.

Démonstration. En effet, on sait d'après la proposition 1.4 que G est isomorphe à $\Gamma(p)$, le plus grand pro-p-quotient de Γ. Par conséquent le résultat se déduit facilement en se rappelant que k_S/k est la pro-p-extension *maximale* de k non ramifiée en dehors de S. □

En d'autres termes, le sous-corps fixé par $\mathcal{G}(\Delta)$ correspond, par la théorie de Galois, au compositum Kk_S/K.

Si l'on suppose de plus que S contient S_p, la conjecture de Leopoldt nous assure la trivialité des multiplicateurs de Schur $H_2(\mathcal{H}, \mathbb{Z}_p)$ pour tout sous-groupe fermé $\mathcal{H}$ de G_S. Le théorème A se déduit alors du théorème 1.13 : pour $\varphi \neq \mathbb{1}$, l'étude de la liberté du module $\mathcal{X}^\varphi$ équivaut à l'étude de la torsion de $(G_{\mathrm{K},S}^{ab})^\varphi$. Dans ce contexte, la proposition 2.3 nous permet d'obtenir :

Corollaire 2.6. *Soit p tel que $p \nmid |\mathrm{Cl}(\mathrm{K})|$ et soit $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$. Alors le module $\mathcal{X}^\varphi$ est $\mathbb{Z}_p[\![G]\!]$-libre si et seulement si*

(i) $\left(\prod_{w \in S \setminus S_p} \mathcal{U}_w\right)^\varphi = \{1\}$, *et*

(ii) $\mathrm{Tor}_{\mathbb{Z}_p} \dfrac{\left(\prod_{w \in S_p} \mathcal{U}_w\right)^\varphi}{\iota(\mathcal{E}_\mathrm{K}^\varphi)} = \{1\}$, *où ι est le plongement diagonal sous-jacent.*

Démonstration. C'est une simple application du théorème A (ou alternativement du théorème 1.13) associée à la proposition 2.3 et au théorème de déploiement 2.4. □

Prenons p *générique*, c'est-à-dire tel que :

- le p-Sylow du groupe des classes $\mathrm{Cl}(\mathrm{K})$ de K est trivial (le premier p n'est pas exceptionnel), et
- pour toute place $w|p$, $\mathrm{K}_w^\times$ ne contient pas de racine primitive p-ème de l'unité.

On a alors :

Corollaire 2.7. *Soit p générique et soit un caractère $\mathbb{Q}_p$-irréductible $\varphi \in \mathrm{Irr}^\bullet(\Delta, \mathbb{Q}_p)$ de Δ tels que les deux φ-composantes suivantes soient triviales :*

(i) $\mathcal{E}_{\mathrm{K}}^{\varphi}$ *et,*

(ii) $\left(\prod_{w\in S\setminus S_p} \mathcal{U}_w\right)^{\varphi}$.

Alors le module $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![G]\!]$-libre.

Démonstration. C'est une conséquence directe du corollaire 2.6. □

Le cas d'une extension à multiplication complexe est particulièrement facile à décrire.

Corollaire 2.8. *Soit* K/k *une extension quadratique à multiplication complexe et soit $p > 2$ générique.*

(i) *Si une place $v \in S\setminus S_p$ se décompose dans* K/k *ou si elle est telle que $\mu_{p^\infty}(\mathrm{k}_v) = \{1\}$, alors $\mathcal{X}^-$ n'est pas $\mathbb{Z}_p[\![G]\!]$-libre.*

(ii) *Supposons le contraire,* i.e. *que pour toute place $v \in S\setminus S_p$, on a $\mu_{p^\infty}(\mathrm{k}_v) \neq \{1\}$ et que v est soit inerte, soit ramifiée dans* K/k. *Alors $\mathcal{X}^-$ est $\mathbb{Z}_p[\![G]\!]$-libre de rang $|S_{\mathrm{k}}|$.*

Démonstration. D'après le théorème 1.13, la liberté du $\mathbb{Z}_p[\![G]\!]$-module $\mathcal{X}^-$ équivaut à la trivialité de $\mathrm{Tor}_{\mathbb{Z}_p}(G_S^{ab})^-$. On utilise ensuite l'isomorphisme de la proposition 2.3 puis le fait que $\mathcal{E}_{\mathrm{K}}^- = \mu_{p^\infty}(\mathrm{K})^-$ (voir par exemple [31, Chapitre 4, Théorème 4.12]) et donc que $\mathcal{E}_{\mathrm{K}}^- = \{1\}$ car p générique, pour arriver à

$$\mathrm{Tor}_{\mathbb{Z}_p}(G_S^{ab})^- \simeq \mathrm{Tor}_{\mathbb{Z}_p}\left(\frac{\prod_{w\in S}\mathcal{U}_w}{\iota(\mathcal{E}_{\mathrm{K}})}\right)^- \simeq \mathrm{Tor}_{\mathbb{Z}_p}(\prod_{w\in S}\mathcal{U}_w)^- \simeq \mathrm{Tor}_{\mathbb{Z}_p}(\prod_{w\in S\setminus S_p}\mathcal{U}_w)^-,$$

et le résultat est alors immédiat. □

Wingberg dans [33] étudie les situations où les groupes $G_{\mathrm{K},S}$ sont de Demushkin, notamment dans le cas à multiplication complexe.

Théorème 2.9 (Wingberg, [33])**.** *Soit* K/k *une extension à multiplication complexe. Supposons qu'il existe une place $w \in S$ telle que $\mu_p(\mathrm{K}_w) \neq \{1\}$. Soit $v|w$. Alors $G_{\mathrm{K},S}$ est un groupe de Demushkin si et seulement si les conditions suivantes sont vérifiées :*

(i) $S_{\mathrm{k}} = S_p = \{v\}$ *et* $|S_{\mathrm{K}}| = 1 + \delta_{\mathrm{K}}$, *où* $\delta_{\mathrm{K}} = 1$ *si* $\mu_p(\mathrm{K}) \neq \{1\}$, 0 *sinon ;*

(ii) $G_{\mathrm{k},S}$ *est un groupe de Demushkin et* $\mu_p(\mathrm{k}_v) \neq \{1\}$ *;*

(iii) $G_{\mathrm{K}}^{S,ab} = \{1\}$.

On en déduit alors le corollaire suivant :

Corollaire 2.10. *Sous les conditions de cette section, supposons que* $G_{\mathrm{K},S}$ *est un groupe de Demushkin. Alors le* $\mathbb{Z}_p[\![G]\!]$*-module* $\mathcal{X}^-$ *est libre.*

Démonstration. D'après le théorème 2.9, le groupe $G_{\mathrm{k},S}$ est de Demushkin, c'est alors une simple application du corollaire 1.20. □

3. Etudes numériques

On se propose de faire quelques simulations numériques dans différentes familles d'extensions galoisiennes $\mathrm{K}/\mathbb{Q}$: cubiques cycliques, cycliques réelles de degré 4 et diédrales de degré 6. Pour une raison de semi-simplicité on a toujours $p \nmid [\mathrm{K} : \mathbb{Q}]$. On suppose la conjecture de Leopoldt vraie dans les extensions en jeu.

Notre étude est centrée sur les nombres premiers p non exceptionnels, c'est-à-dire ceux qui ne divisent pas $|\mathrm{Cl}(\mathrm{K})|$, et l'objet arithmétique à calculer est la φ-partie de la $\mathbb{Z}_p$-torsion du quotient $\prod_{v|p} \mathcal{U}_v/\iota(\mathcal{E}_{\mathrm{K}})$, *i.e.* (à l'exception de $p = 2$) la φ-partie du régulateur normalisé.

Remarque 3.1. On notera que pour $p = 3$ et $p = 5$, les complétés K_w étudiés, $w|p$, ne contiennent pas les racines p-èmes l'unité.

3.1. Le contexte. On va appliquer le corollaire 2.6, redonnons le contexte. Soit p un nombre premier et soit $\mathrm{K}/\mathbb{Q}$ une extension galoisienne de groupe de Galois Δ d'ordre premier à p. On se fixe un caractère $\mathbb{Q}_p$-irréductible non-trivial φ de Δ. On se donne un ensemble fini S de nombres premiers de $\mathbb{Z}$ auquel on ajoute le nombre premier p : ainsi $S_p \subset S$. On pose $\mathcal{G} = G_{\mathrm{K},S}$. On rappelle alors que $\mathcal{G}_\Delta \simeq G_{\mathbb{Q},S}$ et qu'ici $G_{\mathbb{Q},S} \simeq \mathbb{Z}_p$ si et seulement si pour tout premier $\ell \in S \backslash S_p$, il vient $\ell \not\equiv 1 \pmod p$. Remarquons que le groupe $G_{\mathbb{Q},S}$ n'est pas p-adique analytique pour S assez grand. On prend $\mathcal{H} = \mathcal{G}(\Delta) = \mathrm{Gal}(\mathrm{K}\mathbb{Q}_S/\mathrm{K})$, puis $\mathcal{X} = \mathcal{H}^{ab}$. Enfin, on suppose que les premiers $\ell \in S \backslash S_p$ n'apportent pas d'obstruction à la liberté de $\mathcal{X}^\varphi$, *i.e* que $\left(\prod_{w|\ell \in S\backslash S_p} \mathcal{U}_w\right)^\varphi = \{1\}$.

Supposons de plus p non exceptionnel. Par le choix des ℓ, il vient que $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![G_{\mathbb{Q},S}]\!]$-libre si et seulement si

$$\mathrm{Tor}_{\mathbb{Z}_p}(G_{S,\mathrm{K}}^{ab})^{\varphi} \simeq \mathrm{Tor}_{\mathbb{Z}_p}\Big(\frac{\big(\prod_{w|p}\mathcal{U}_w\big)^{\varphi}}{\iota(\mathcal{E}_{\mathrm{K}}^{\varphi})}\Big) = \{1\}.$$

Si la φ-composante $\mathcal{E}_{\mathrm{K}}^{\varphi} = \langle x_1, \cdots, x_d\rangle$ de $\mathcal{E}_{\mathrm{K}}$ est de $\mathbb{Z}_p$-rang $d > 0$, alors

$$\mathrm{Tor}_{\mathbb{Z}_p}\frac{\big(\prod_{w\in S_p}\mathcal{U}_w\big)^{\varphi}}{\iota(\mathcal{E}_{\mathrm{K}}^{\varphi})} \neq \{1\}$$

si et seulement si il existe $a_1, \cdots, a_d \in \{0, \cdots, p-1\}$, *non tous nuls*, tels que

$$\forall w \in S_p,\ \iota_w(x_1^{a_1}\dots x_d^{a_d}) \in \mathcal{U}_w^p,$$

où ι_w est le plongement de K dans $\mathcal{U}_w$. Si l'on suppose par exemple $a_1 \neq 0$, par la relation de Bézout entre a_1 et p, on se ramène à tester la condition $\iota_w(x_1x_2^{a_2}\dots x_d^{a_d}) \in \mathcal{U}_w^p$, pour tout $w \in S_p$, quand les puissances a_i varient dans $[\![0, p-1]\!]$.

Remarque 3.2. Remarquons qu'il nous faut des générateurs de $\mathcal{E}_{\mathrm{K}}$, ce qui est moins "fin" que des générateurs de E_{K}.

Plaçons-nous dans le cadre suivant : supposons que $\mathcal{E}_{\mathrm{K}}^{\varphi} = \langle\varepsilon\rangle_{\mathbb{Z}_p}$ est engendré par une unité ε de K. Alors, pour p générique, $\mathcal{X}^{\varphi}$ est non-libre si et seulement si $\iota_w(\varepsilon) \in \mathcal{U}_w^p$ pour toute place $w \in S_p$. Cette dernière condition est alors facile à tester : c'est une simple condition de congruence dans K impliquant une certaine relation entre les unités x_i. Précisons à ce niveau que tout ceci s'adapte parfaitement au cas où le caractère $\mathbb{Q}_p$-irréductible φ s'écrit $\varphi = \sum_{\psi|\varphi}\psi$, où les ψ sont des caractères $\mathbb{C}_p$-irréductible de degré 1 ; *in fine*, cela revient aussi à tester si une certaine unité est une puissance p-ème localement en toutes les places $w|p$.

Pour les trois situations à venir, nous avons fait le choix suivant : partir d'un polynôme P dont les racines forment une base des unités du corps K. Dans ce cas, et quand $\mathcal{E}_{\mathrm{K}}^{\varphi} = \langle\varepsilon\rangle$ (ou éventuellement quand $\mathcal{E}_{\mathrm{K}}^{\psi}$ est monogène), la condition à tester se réduit à une simple condition de congruence dans $\mathbb{Z}$ (à l'exception d'un ensemble de premiers p bien localisés).

En effet, tout d'abord, pour $p > 2$ montrer que ε est une puissance p-ème localement en $w \in S_p$ équivaut à montrer que

$$w(\varepsilon^{a_p} - 1) \geqslant e + 1, \tag{10}$$

où $a_p = p^f - 1$, e et f étant respectivement les indices de ramification et d'inertie de p dans $\mathrm{K}/\mathbb{Q}$ (dans notre étude on a toujours $p > e+1$) et où w est la valuation associée à la place w. Ainsi lorsque $p > 2$ est non ramifié, montrer que ε est une puissance p-ème localement en toutes les places $w \in S_p$ équivaut à montrer que

$$\varepsilon^{a_p} - 1 \equiv 0 \pmod{p^2}. \tag{11}$$

Ensuite, dans les situations cycliques, $\varepsilon = u(x)$ est une fonction polynomiale en une racine x de P à coefficients dans $\mathbb{Q}$. La congruence (11) dans $\mathcal{O}_\mathrm{K}$ peut alors être vue dans $\mathbb{Z}$ de la façon suivante. En s'assurant que $p \nmid \mathrm{Disc}(P)$, on peut écrire

$$\varepsilon^{a_p} - 1 = Q(x) + p^2 y,$$

où $Q = \lambda_0 + \lambda_1 X \cdots + \lambda_{n-1} X^{n-1} \in \mathbb{Z}[X]$, $n = [\mathrm{K} : \mathbb{Q}]$, et où $y \in \mathcal{O}_\mathrm{K}$. Il est alors immédiat que (11) équivaut à vérifier que Q est trivial dans le quotient $\mathbb{Z}[X]/(P, p^2)$

Enfin, dans la famille d'extensions diédrales, par un résultat de Maus [22], on aura $\mathcal{O}_\mathrm{K} = \mathbb{Z}[x_1, x_2]$ avec $P(x_i) = 0$. Là aussi, à l'exception de premiers p bien localisés, on peut écrire

$$\varepsilon^{a_p} - 1 = Q(x_1, \sqrt{\mathrm{Disc}(P)}) + p^2 y,$$

où $Q = \sum_{0 \leqslant i \leqslant 2, 0 \leqslant j \leqslant 1} \lambda_{i,j} X^i Y^j \in \mathbb{Z}[X, Y]$, et où $y \in \mathcal{O}_\mathrm{K}$. Alors la congruence (11) équivaut à la trivialité de Q dans le quotient $\mathbb{Z}[X, Y]/(P(X), Y^2 - \mathrm{Disc}(P), p^2)$.

3.2. Extensions cubiques cycliques. Soit $p \neq 3$ et soit un polynôme P de degré 3 irréductible sur $\mathbb{Q}$ définissant un corps cubique cyclique que l'on note K.

On fait le choix pour la suite d'ordonner les racines de P par ordre croissant : $\varepsilon_1 < \varepsilon_2 < \varepsilon_3$, et de prendre pour générateur du groupe $\Delta = \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ le morphisme σ défini par $\sigma(\varepsilon_1) = \varepsilon_2$ et $\sigma(\varepsilon_2) = \varepsilon_3$.
Supposons que les racines de P engendrent $\mathcal{E}_\mathrm{K}/\langle \pm 1 \rangle$.
Le groupe Δ a trois caractères $\mathbb{C}_p$-irréductibles $\mathbb{1}$, φ et φ^2.

3.2.1. *Quand* 3 *divise* $p-1$. Les caractères φ et φ^2 sont définis sur $\mathbb{Q}_p$. Soit $\zeta \in \mathbb{Q}_p$ une racine primitive cubique de l'unité. Fixons φ tel que $\varphi(\sigma) = \zeta$ et posons

$$u_\varphi = \varepsilon_1 \varepsilon_2^{-\zeta} \quad \text{et} \quad u_{\varphi^2} = \varepsilon_1 \varepsilon_2^{-\zeta^2}.$$

Alors $\sigma(u_\varphi) = u_\varphi^\zeta$, $\sigma(u_{\varphi^2}) = u_{\varphi^2}^{\zeta^2}$ et, ainsi, $\mathcal{E}_\mathrm{K}^\varphi = \langle u_\varphi \rangle$ et $\mathcal{E}_\mathrm{K}^{\varphi^2} = \langle u_{\varphi^2} \rangle$.

Nos résultats montrent que pour p générique (et p non ramifié), la φ-composante $\mathcal{X}^{\varphi}$ est libre, en fait triviale ici, si et seulement si

$$\left(\varepsilon_1\varepsilon_2^{-a}\right)^{a_p} - 1 \not\equiv 0 \pmod{p^2},$$

où $a \in \{1, \cdots, p-1\}$ est tel que $\zeta \equiv a \pmod{p}$. Comme nous l'avons vu, cette congruence se teste facilement. En effet, à l'exception de quelques nombres premiers p (en fait ceux divisant $\mathrm{Disc}(P)$), l'élément $\left(\varepsilon_1\varepsilon_2^{-a}\right)^{a_p} - 1$ peut être vu, modulo $p^2\mathcal{O}_{\mathrm{K}}$, comme un polynôme Q de $\mathbb{Z}[X]$, et la condition "$\left(\varepsilon_1\varepsilon_2^{-a}\right)^{a_p} - 1 \not\equiv 0 \pmod{p^2}$" équivaut à "$Q \not\equiv 0 \pmod{(P, p^2)}$".

C'est cette dernière condition que l'on va tester de façon intensive. On note R le couple $[\varepsilon_1, \varepsilon_2]$. Pour un premier p donné, il suffit alors de considérer un relèvement a d'une racine primitive cubique mod p puis de calculer les congruences. Le programme (avec PARI/GP) est donc plutôt simple. On note toujours f l'indice d'inertie de p dans $\mathrm{K}/\mathbb{Q}$.

```
torsion(P,R,p,f,a)=
{my(Rmodp2,T);
T=vector(2);
E1=Mod(Mod(R[1],P),p^2);
E2inv=Mod(Mod(R[2]^(-1),P),p^2);
T[1]=lift((E1*E2inv^a)^(p^f-1)-1)==Mod(0,p^2);
T[2]=lift((E1*E2inv^(a^2))^(p^f-1)-1)==Mod(0,p^2)
T;}
```

Ce code renvoie un couple $[T1, T2]$, où chacune des composante est 1 ou 0 suivant si $Q \equiv 0 \pmod{(P, p^2)}$ ou non. On peut ensuite faire varier les premiers p.

Balady dans [1] donne plusieurs familles de polynômes, généralisant celle de Kishi [17], qui fournissent une base d'unités de K. Ils sont construits de la manière suivante : soient f et g deux polynômes à coefficients entiers et soient $\lambda = \left(f^3 + g^3 + 1\right)/fg$ puis $a = 3\left(f^2 + g^2 - fg\right) - \lambda\left(f + g\right)$. Considérons la famille de polynômes $P_n = X^3 + a(n)X^2 + \lambda(n)X - 1, n \in \mathbb{Z}$. Alors sous les hypothèses :

(α) λ est un polynôme à coefficients entiers,

(β) $n \neq -1$,

(γ) $3a(n) + \lambda(n)^2$ est sans facteurs carrés,

les polynômes P_n déterminent des corps cubiques cycliques K_n (noté également K) dont les racines engendrent $E_{\mathrm{K}}/\langle \pm 1 \rangle$.

Introduisons quelques notations pour présenter nos calculs. Lorsque P est donné, notons respectivement $\mathcal{D}_{disc}$ et $\mathcal{D}_{Cl}$ l'ensemble des diviseurs de $\mathrm{Disc}(P)$

et du nombre de classes du corps K (le corps cubique de polynôme P). Soit ensuite $\mathbb{P}$ $(= \mathbb{P}_{\mathrm{K}})$ l'ensemble des nombres premiers p vérifiant : (i) $p \equiv 1 (\mathrm{mod}\ 3)$, (ii) $p \notin \mathcal{D}_{Cl} \cup \mathcal{D}_{disc}$. Posons alors

$$\mathcal{F}_{nl}(X) := \{p \in \mathbb{P},\ p \leqslant X,\ \mathcal{X}^{\varphi} \text{ ou } \mathcal{X}^{\varphi^2} \text{ non libre}\}.$$

À p fixé, le caractère irréductible φ est déterminé par la donnée d'un élément a de $\{0, \cdots, p-1\}$, et pour $p \in \mathcal{F}_{nl}(X)$, on renseigne en indice l'entier a associé à la composante non-libre (non-triviale ici).

• Prenons la famille de polynômes P_n donnée par Balady à partir de $f(n) = -n^2$ et $g(n) = n^3 - 1$. Pour $1 \leqslant n \leqslant 100$, on trouve 51 polynômes vérifiant les conditions (α), (β) et (γ). Le tableau en annexe A.2.1 donne les résultats obtenus pour $X = 23 \times 10^7$ (et ces 51 corps cubiques). Notons que l'on n'a aucun exemple où les deux composantes ne sont pas triviales (simultanément).

Remarque 3.3. Afin de réduire au maximum les temps de calcul, la liste des relèvements des racines cubique modulo p pour tous les premiers inférieurs à une certaine borne ($X = 23 \times 10^7$ pour nous) est calculée à part. Lorsque, à n fixé, nous faisons varier p de 1 à 10^6, ce principe nous permet de diviser le temps de calcul par plus de 60.

Dans ces calculs, à n fixé, deux ensembles de premiers sont exclus : $\mathcal{D}_{disc}$ et l'ensemble des premiers exceptionnels $\mathcal{D}_{Cl}$. Il est néanmoins possible de faire le calcul différemment et de conclure pour ces nombres premiers grâce aux algorithmes de Gras [9] et Pitoun-Varescon [27] qui utilisent les calculs du corps de classes de PARI/GP. En effet, notre hypothèse sur l'ensemble S fait que tout se passe au niveau des complétés p-adiques et ainsi, finalement, tester la liberté des composantes de $\mathcal{X}$ équivaut à tester la p-rationalité du corps K (ce que testent ces algorithmes) : le défaut de non rationalité de K est localisé en φ ou/et φ^2 (car $\mathbb{Q}$ est p-rationnel).

(a) Pour les premiers $p \in \mathcal{D}_{disc} \backslash \mathcal{D}_{Cl}$, le résultat est immédiat : dans l' intervalle étudié ($n \leqslant 100$ vérifiant (α), (β) et (γ)), les corps sont p-rationnels.

(b) Pour les premiers $p \in \mathcal{D}_{Cl}$, aucun des 51 corps n'est p-rationnel. Concentrons-nous sur la trivialité du régulateur normalisé :

- Quand p n'est pas ramifié dans K/$\mathbb{Q}$, le régulateur normalisé est non-trivial uniquement lorsque : $(n, p_a) \in \{(11, 7_4), (16, 7_4), (17, 7_{4^2}), (49, 7_4), (67, 7_4)\}$. À noter que $d_p \mathrm{Tor}_{\mathbb{Z}_p} G^{ab}_{\mathrm{K},S_p} = 1$ pour $(11, 7)$ et $(67, 7)$, et que $d_p \mathrm{Tor}_{\mathbb{Z}_p} G^{ab}_{\mathrm{K},S_p} = 2$ pour les couples $(16, 7)$, $(17, 7)$ et $(49, 7)$.
- Quand p est ramifié : le régulateur normalisé est trivial dans tous les cas.

Remarque 3.4. Comme on l'a expliqué plus tôt, les algorithmes de Pitoun-Varescon et de Gras déterminent le module de torsion $\mathrm{Tor}_{\mathbb{Z}_p} G_{S_p}^{ab}$, testant ainsi si un corps donné est, ou non, p-rationnel pour un premier p fixé. Nous avons choisi pour nos calculs d'utiliser d'abord notre code, puis de traiter les cas particuliers avec l'algorithme de Pitoun-Varescon. Nous calculons donc avec PARI/GP le nombre de classes de K puis faisons varier p où les calculs se résument à des congruences dans $\mathbb{Z}$ alors que l'algorithme de Pitoun-Varescon nécessite le calcul d'un corps de classes de rayon pour chaque premier p. À titre de comparaison, voici les temps mis par les deux programmes pour le polynôme $P = X^3 + 309X^2 - 10X - 1$ (polynôme de Balady, $n = 2$) lorsque l'on fait varier le premier p de 1 à 10^6 : avec l'algorithme de Pitoun-Varescon on obtient la liste des corps non p-rationnels en plus d'une heure, alors que notre algorithme renvoie la liste des composantes non-libres en 4.808ms (en calculant les racines cubiques au préalable). Pour être complet, notons que sur cet exemple l'algorithme de Gras est plus rapide que celui de Pitoun-Varescon (un peu moins d'une heure).

• Prenons maintenant la famille de Lecacheux [19], que l'on retrouve à partir des polynômes de Balady pour $f(n) = -1$ et $g(n) = -n$. Pour $1 \leqslant n \leqslant 100$, on trouve 25 polynômes vérifiant les conditions voulues. Les tableaux en annexe A.2.2 donnent les résultats obtenus pour $X = 23 \times 10^7$ (et $1 \leqslant n \leqslant 100$). Là encore, on traite à part en utilisant l'algorithme de Pitoun-Varescon les premiers de $\mathcal{D}_{disc}$ et de $\mathcal{D}_{Cl}$.

(a) Dans les intervalles étudiés, pour chaque premier $p \in \mathcal{D}_{disc} \backslash \mathcal{D}_{Cl}$, le corps est p-rationnel, à l'exception des trois situations suivantes : $n = 50$, $n = 62$ et $n = 76$ pour le nombre premier $p = 7$. On peut alors faire le calcul directement dans le corps de nombres pour déterminer quelle φ-composante est non-libre. On voit que pour $n = 62$ et $n = 76$, la composante $\mathcal{X}^{\varphi}$ est non-libre pour φ donné par la racine cubique 4 mod 7 (l'autre composante est libre). Détaillons le cas $n = 50$. Ici $u_{\varphi}^{a_p} = (\varepsilon_1 \varepsilon_2^{-4})^6$ et $u_{\varphi^2}^{a_p} = (\varepsilon_1 \varepsilon_2^{-16})^6$ et un calcul avec PARI/GP donne $\varepsilon_2 = -2451\varepsilon_1^2/49 + 6009802\varepsilon_1 + 6007352/49$. Enfin, on détermine $v_{\mathfrak{p}_i}(u_{\varphi^j}^6 - 1)$ avec la fonction `idealval` et on voit qu'aucune des composantes $\mathcal{X}^{\varphi^j}$ n'est libre (non triviale ici). Sur tous les exemples étudiés jusqu'à présent, c'est le seul cas où les deux composantes non triviales sont simultanément non-libres.

(b) Pour $p \in \mathcal{D}_{Cl}$, aucun corps n'est p-rationnel dans les intervalles étudiés. En revanche, les seules situations où le régulateur normalisé est non-trivial sont les suivantes : $(n, p_a) \in \{(34, 7_4), (68, 13_{3^2}), (98, 7_4)\}$.

3.2.2. *Quand* 3 *ne divise pas* $p - 1$. Cette condition est plus contraignante que la précédente puisqu'elle force la p-torsion de G_{K,S_p}^{ab} à être de p-rang pair.

Prenons $p > 3$. Un raisonnement identique à celui effectué dans le cas précédent montre que la trivialité de la composante $\mathcal{X}^{\varphi+\varphi^2}$ équivaut à la condition $\left(\varepsilon_1^2\varepsilon_2\right)^{a_p} - 1 \not\equiv 0 \pmod{p^2}$.

• Pour $f(n) = -n^2$, $g(n) = n^3 - 1$, $p < 10^9$ et $n \leqslant 100$ vérifiant (α), (β) et (γ), le seul cas non-trivial trouvé est :

- $n = 62, p = 23$ $(f = 1)$.

• Pour $f(n) = -1$, $g(n) = -n$, $p < 10^9$ et $n \leqslant 100$ vérifiant (α), (β) et (γ), les seuls cas non-triviaux trouvés sont :

- $n = 38, p = 5$ $(f = 2)$;
- $n = 88, p = 5$ $(f = 2)$.

Ici encore l'algorithme de Pitoun-Varescon permet d'étudier la liberté des φ-composantes pour chaque valeur de $p \in \mathcal{D}_{disc} \cup \mathcal{D}_{Cl}$. Dans le premier cas ($f = -n^2$, $g = n^3 - 1$) tous les corps sont p-rationnels (pour $p > 3$), donc toutes les composantes restantes sont en fait libres. Dans le second cas ($f = -1$, $g = -n$), on trouve seulement deux autres situations où le corps n'est pas p-rationnel pour lesquels un calcul dans le corps de nombres permet de conclure : pour $(n, p) \in \{(26, 5), (76, 5)\}$, la $(\varphi + \varphi^2)$-composante de $\mathcal{X}$ n'est pas triviale (pour ces deux cas, $p \in \mathcal{D}_{disc} \backslash \mathcal{D}_{\mathrm{Cl}}$).

Enfin, traitons rapidement le cas $p = 2$. Dans les familles étudiées (2 est inerte), on peut vérifier que l'obstruction à la non-trivialité de $\mathcal{X}^{\varphi+\varphi^2}$ provient à chaque fois du groupe des classes.

Exemple 3.5. Soit l'extension cubique cyclique $\mathrm{K}/\mathbb{Q}$ de polynôme $P = X^3 + 12286733X^2 - 9970X - 1$ (polynôme de Balady, $n = 10$). Alors pour $p < 3 \times 10^7$, le régulateur normalisé de K est trivial à l'exception des nombres premiers 3, 43 et 14783491. Pour $p = 43$, c'est la φ-composante associée à la racine cubique $\zeta \equiv 6^2 (\mathrm{mod}\ 43)$ qui est non-triviale. Pour $p = 14783491$, c'est la φ-composante associée à la racine cubique $\zeta \equiv 4865581 \pmod{p}$. A noter que $p = 3$ est à part pour notre étude à cause de l'hypothèse de semi-simplicité.

3.3. Extensions cycliques totalement réelles de degré 4. On se donne p un nombre premier impair. Soit $\zeta \in \mathbb{C}_p$ une racine primitive quatrième de l'unité.

Soit P un polynôme irréductible de degré 4 et K son corps de décomposition, qu'on suppose quartique cyclique et totalement réel. On note Δ le groupe de Galois de l'extension $\mathrm{K}/\mathbb{Q}$ et on fixe σ un générateur de Δ. On ordonne alors les racines ε_i de P de sorte que σ soit donné par le cycle $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$. Le groupe

Δ a quatre caractères $\mathbb{Q}_p(\zeta)$-irréductibles de degré 1 : $\mathbb{1}$, φ, φ^2 et φ^3, où φ est défini par $\varphi(\sigma)=\zeta$.
Supposons alors que les racines de P engendrent le groupe $\mathcal{E}_K$.

Lorsque $p\equiv 1 \pmod 4$, les caractères φ^i sont en fait $\mathbb{Q}_p$-irréductibles. On vérifie qu'en posant

$$u_\varphi=\varepsilon_1\varepsilon_2^{1-\zeta}\varepsilon_3^{-\zeta},\quad u_{\varphi^2}=\varepsilon_1\varepsilon_3 \ \text{ et } \ u_{\varphi^3}=\varepsilon_1\varepsilon_2^{1+\zeta}\varepsilon_3^{\zeta},$$

il vient $\mathcal{E}_{\mathrm{K}}^{\varphi}=\langle u_\varphi\rangle$, $\mathcal{E}_{\mathrm{K}}^{\varphi^2}=\langle u_{\varphi^2}\rangle$ et $\mathcal{E}_{\mathrm{K}}^{\varphi^2}=\langle u_{\varphi^3}\rangle$. Pour p non-ramifié dans l'extension $\mathrm{K}/\mathbb{Q}$, la non-liberté (ou non-trivialité ici) du module $\mathcal{X}^{\varphi^i}$ équivaut donc à étudier la congruence : $u_{\varphi^i}^{a_p}\equiv 1 \pmod{p^2}$, où $a_p=p^f-1$, avec f le degré résiduel de p dans l'extension $\mathrm{K}/\mathbb{Q}$.

Si maintenant $p\equiv 3 \pmod 4$, le groupe Δ n'a que deux caractères $\mathbb{Q}_p$-irréductibles non triviaux qui sont φ^2 et $\varphi+\varphi^3$ et la non-liberté du module $\mathcal{X}^{\varphi+\varphi^3}$ équivaut dans ce cas à la congruence $\varepsilon_1^2\varepsilon_2^2\varepsilon_3\equiv 1 \pmod{p^2}$ (ici $p>5$).

Dans [2], Balady et Washington exhibent une famille de polynômes

$$P_s=X^4+4(s^3-s^2+2s-1)X^3+6(-s^2-1)X^2+4X+1,$$

$s\in\mathbb{Z}^*$, dont le corps de décomposition K_s est un corps totalement réel cyclique de degré 4 et dont les racines engendrent soit les unités de K_s soit un sous-groupe d'indice 5 dès que : (α') $3s^2-4s+4$ est un carré, et (β') s^2+2 est sans facteurs carrés.

Cependant, les conditions sur le paramètre s sont très restrictives : pour $|s|<10^6$, il n'y a que les entiers -34272, -2460, -12, 48, 660, 127908 qui vérifient (α') et (β') à la fois.

Lors de la construction de la famille $(P_s)_s$, Balady et Washington choisissent pour générateur σ de Δ la matrice d'ordre 4 de $PGL_2(\mathbb{Z})$

$$\begin{pmatrix} f & -1 \\ \dfrac{f^2+g^2}{2} & -g \end{pmatrix},$$

où $f=\dfrac{2+\sqrt{3s^2-4s+4}}{2}$ et $g=\dfrac{2-\sqrt{3s^2-4s+4}}{2}$. Son action sur les racines de P_s donne alors immédiatement

$$\varepsilon_2=\frac{f\varepsilon_1-1}{\dfrac{f^2+g^2}{2}\varepsilon_1-g},\quad \varepsilon_3=\frac{(f+g)\varepsilon_1-2}{(f^2+g^2)\varepsilon_1-g-f} \ \text{ et } \ \varepsilon_4=\frac{g\varepsilon_1-1}{\dfrac{f^2+g^2}{2}\varepsilon_1-f},$$

et le générateur σ du groupe Δ est bien défini par le cycle $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$.

On voit encore une fois que l'hypothèse de congruence peut se tester directement dans $\mathbb{Z}[X]/(P_s)$ de façon très simple.

Les formules données plus haut pour exprimer les racines ε_2 et ε_3 du polynôme P ont des dénominateurs et les diviseurs premiers de ces dénominateurs doivent être traités à part. On note par $\mathcal{D}$ l'ensemble de ces premiers. Posons

$$\mathcal{F}_{nl}(X) := \{p \text{ premier}, p \notin \mathcal{D} \cup \mathcal{D}_{cl} \cup \mathcal{D}_{disc},\ 5 < p \leqslant X,\ \exists i \in \{1,2,3\},\ \mathcal{X}^{\varphi^i} \neq \{0\}\}.$$

Le programme PARI/GP utilisé pour déterminer si les φ-composantes sont, ou non, libres (*i.e.* triviales ici) est construit sur le même modèle que celui de la section 3.2. Les résultats obtenus en faisant varier p de 1 à $X = 15 \times 10^7$ sous la condition $p \equiv 1 \pmod 4$ sont présentés dans le tableau en annexe A.1. Le caractère φ est donné par la congruence de ζ modulo p, que l'on note a, et comme pour le cas cubique, pour chaque premier $p \in \mathcal{F}_{nl}(X)$, on précise en indice a^k, la composante $\mathcal{X}^{\varphi^k}$ non-triviale ; à noter que quand $k = 2$, cela signifie que l'obstruction provient du sous-corps quadratique réel.

Lorsque l'on fait varier p sous la condition $p \equiv 3 \pmod 4$ dans le même intervalle, on ne trouve que cinq situations non-libres : $(-34272, 37511)$, $(-2460, 491)$, $(660, 25652023)$, $(127908, 3)$, $(1781520, 7)$. Dans chacun de ces cas, l'obstruction provient du sous-corps quadratique réel (via le caractère φ^2).

Enfin, regardons via l'algorithme de Pitoun-Varescon (ou alternativement de Gras) les premiers mis de côté.

(a) Les corps sont tous p-rationnels pour $p \in \mathcal{D} \cup \mathcal{D}_{disc}$.

(b) Pour $p \in \mathcal{D}_{Cl} \backslash \mathcal{D} \cup \mathcal{D}_{disc}$: aucune situation n'est p-rationnelle, mais seuls les cas $(n, p_a) \in \{(-92604732, 5_{3^2}), (-92604732, 37_{6^1}), (1781520, 5_{3^1})\}$ ont un régulateur normalisé non-trivial.

3.4. Extensions diédrales. Soit la famille $P_n = X^3 + nX + 1$, $n \in \mathbb{N}$. Notons $d_n = -4n^3 - 27 < 0$ le discriminant du polynôme P_n que l'on suppose sans facteurs carrés ; par [6], on sait que les entiers n vérifiant cette condition sont de densité positive. Soit le corps quadratique imaginaire $\mathrm{F}_n = \mathbb{Q}(\sqrt{d_n})$ et soit ε une racine réelle de P_n. On note K_n le corps $\mathbb{Q}(\sqrt{d_n}, \varepsilon)$. Cette fois-ci le corps de décomposition $\mathrm{K} = \mathrm{K}_n$ de P_n est de groupe de Galois Δ isomorphe à S_3. Soit $p \geqslant 5$. Le groupe Δ a deux représentations $\mathbb{Q}_p$-irréductibles de degré 1 (la représentation triviale $\mathbb{1}$ et une représentation ψ), et une représentation $\mathbb{Q}_p$-irréductible φ de degré 2.

Le groupe des unités $\mathcal{E}_{\mathrm{K}}$ a pour caractère φ et, pour p générique, le $\mathbb{Z}_p[\Delta]$-module $\prod_{w \in S_p} \mathcal{U}_w$ a pour caractère $\mathbb{1} + \psi + 2\varphi$.

Choisissons ensuite les premiers $\ell \neq p$ de S tous congrus à 1 modulo p et tels que P_n est irréductible modulo ℓ. Pour $\ell \in S\backslash S_p$, l'action de Δ sur $\prod_{w|\ell}\mathcal{U}_w$ a pour caractère $\mathbb{1}+\psi$. Par conséquent la composante $(G_{S,\mathrm{K}}^{ab})^{\psi}$ est $\mathbb{Z}_p$-libre si et seulement si $S = S_p$ et dans ce cas, $\mathcal{X}^{\psi} = \{0\}$. La situation intéressante se trouve donc dans l'étude de $\mathcal{X}^{\varphi}$. Pour $\ell \in S\backslash S_p$, $(\prod_{w|\ell}\mathcal{U}_w)^{\varphi} = \{1\}$, on est donc dans le cadre du corollaire 2.6. En particulier si le module $\mathcal{X}^{\varphi}$ est $\mathbb{Z}_p[\![G_{\mathbb{Q},S}]\!]$-libre, alors il est libre de rang 2.

Notons ε_2 une seconde racine de P_n. Dans [21], l'auteur utilise les estimations données par Cusick dans [4] pour minorer le régulateur du corps $\mathbb{Q}(\varepsilon)$, ce qui permet de montrer que ε est une unité fondamentale de $\mathbb{Q}(\varepsilon)$. Un raisonnement sur les normes permet ensuite de montrer que $\{\varepsilon, \varepsilon_2\}$ forme une $\mathbb{Z}_p$-base des unités de K_n. Ainsi, suivant les calculs de la situation cubique cyclique, il nous faut simplement tester la condition (pour p non ramifié)

$$\left(\varepsilon\varepsilon_2^2\right)^{a_p} \equiv 1 \pmod{p^2},$$

où comme précédemment, $a_p = p^f - 1$, f étant le degrés résiduel de p dans $\mathrm{K}_n/\mathbb{Q}$. La forme particulière du polynôme considéré nous donne des relations très simples entre les racines de P ($\varepsilon_2 = \dfrac{\sqrt{d_n}}{2(20n^2-d_n)}(12n\varepsilon^2 - 9\varepsilon + 16n^2) - \dfrac{\varepsilon}{2}$, par exemple). Le programme permettant de tester la condition de congruence dans $\mathcal{O}_{\mathrm{K}}$ est alors facile à mettre en oeuvre : ici, ε_2 s'écrit sous la forme d'un polynôme $u(\varepsilon, \sqrt{d_n})$, et comme expliqué dans la section 3.1, la congruence se lit dans le quotient $\mathbb{Z}[X,Y]/(P(X), Y^2 - d_n, p^2)$.

Le polynôme P_n est irréductible et de discriminant sans facteur carré pour 61 valeurs de n comprises entre 2 et 100. En faisant varier p de 5 à 10^9 dans chacune de ces situations, les seuls cas où la φ-composante de $\mathcal{X}$ n'est pas libre sont :

- $n = 25$, $p = 5$ $(f = 2)$;
- $n = 49$, $p = 7$ $(f = 1)$;
- $n = 50$, $p = 5$ $(f = 2)$;
- $n = 98$, $p = 7$ $(f = 1)$.

Voir [28] pour le programme détaillé.

Ici encore nous avons écarté des ensembles de nombres premiers : $\mathcal{D}_{Cl}$, $\mathcal{D} := \{p \mid 20n^2 - d_n\}$ et $\mathcal{D}_{ram}$, où $\mathcal{D}_{ram}$ désigne l'ensemble des nombres premiers ramifiés dans $\mathrm{K}/\mathbb{Q}$.

(a) Pour $p \in \mathcal{D}$, on trouve, pour n variant de 2 à 100 (tel que d_n soit sans facteurs carrés) et p inférieur à 10^8, deux corps non-7-rationnel : pour $n = 52$ et

$n = 80$. Dans ces deux cas, on vérifie que F_n n'est pas 7-rationnel. D'un autre côté, un calcul montre que $d_p \mathrm{Tor}_{\mathbb{Z}_p} G^{ab}_{\mathrm{K},S_7} = 1$, et ainsi, $\left(\mathrm{Tor}_{\mathbb{Z}_p} G^{ab}_{\mathrm{K},S_7}\right)^{\varphi} = \{1\}$.

(b) Pour les premiers p de $\mathcal{D}_{Cl}\backslash\mathcal{D}$, on trouve seulement cinq situations non p-rationnelles : $(n,p) \in \{(19,7),(31,5),(32,7),(97,5),(100,5)\}$. Ici, seul le couple $(100,5)$ a un régulateur normalisé non trivial (en la composante φ).

(c) Le corps de nombres K est p-rationnel pour tous les premiers p ramifiés dans $\mathrm{K}/\mathbb{Q}$.

Remarque 3.6. La très faible proportion de couples (n,p) pour lesquels on détecte une composante non-libre subsiste pour d'autre valeurs de n : lorsque l'on fait varier à la fois l'entier n et le premier p de 1 à 10^5, on balaye 62486 corps, et on teste plus de 56×10^8 composantes non-triviales associées à ces corps de nombres pour finalement ne trouver que 4041 couples (n,p) pour lesquels une des composantes est non-libre, ce qui revient à moins de $7.2 \times 10^{-5}\%$ des cas seulement ! Notons enfin que pour $313 < p < 10^5$, les composantes étudiées (*i.e.* non-triviales) sont toutes libres.

Annexe A. Résultats numériques

A.1. Cas cyclique de degré 4. Voir la section 3.3.

s	$\mathcal{D}$	$\mathcal{D}_{Cl}$	$\mathcal{D}_{disc}$	$\mathcal{F}_{nl}(15 \times 10^7)$
-92604732	$\{2, 59, 521, 2609\}$	$\{2, 3, 5, 13, 37, 53, 251, 18464557\}$	$\{2, 59, 521, 1889, 2609, 2857, 23561, 33721\}$	$\{1193_{186^2}, 3529_{808^1}, 3663533_{220189^3}, \}$
-34272	$\{2, 67, 443\}$	$\{2, 3, 5, 131, 1597\}$	$\{2, 67, 443, 587284993\}$	$\{193_{81^1}, 313_{25^3}, 389_{115^3}, 88969_{21228^1}, 3019229_{14846^3}, 14771837_{6095056^1}\}$
-2460	$\{2, 2131\}$	$\{2, 3, 5, 13\}$	$\{2, 113, 2131, 26777\}$	$\varnothing$
-12	$\{2, 11\}$	$\{2\}$	$\{2, 11, 73\}$	$\{17_{4^2}, 19363829_{8692313^3}, 12690513_{3461050^3}, 26900513_{5491405^3}\}$
48	$\{2, 41\}$	$\{2\}$	$\{2, 41, 1153\}$	$\{13_{5^1}, 379849_{180001^3}, 763597_{309179^2}, 2152957_{253167^2}\}$
660	$\{2, 571\}$	$\{2, 5, 13\}$	$\{2, 353, 571, 617\}$	$\{349_{136^2}, 1949_{589^1}, 9137_{1286^3}\}$
127908	$\{2, 110771\}$	$\{2, 7, 13, 17, 9337\}$	$\{2, 73, 110771, 112057921\}$	$\{5_{3^3}, 29_{12^1}, 1117_{214_3}, 117889_{38118^2}\}$
1781520	$\{2, 1542841\}$	$\{2, 5, 11, 47, 677208593\}$	$\{2, 1542841, 1586906755201\}$	$\{29_{12^2}\}$

A.2. Cas cyclique de degré 3.

A.2.1. *Famille de polynômes de Balady.* Pour les notations, voir la section 3.2.1.

n	$\mathcal{D}_{disc}$	$\mathcal{D}_{Cl}$	$\mathcal{F}_{nl}(23\times 10^7)$
1	$\{19\}$	$\varnothing$	$\{67_{29^2}, 193_{84}, 337_{128^2}, 7321_{308^2}\}$
2	$\{11, 13, 79\}$	$\{3\}$	$\{19_{72}, 439_{171}, 2887_{698^2}, 59060857_{26994113}, 122648623_{5895446}\}$
4	$\{13, 19, 79, 571\}$	$\{3, 13\}$	$\varnothing$
7	$\{17, 23, 2383, 3769\}$	$\{3, 7, 223\}$	$\{199_{92}, 277_{116}\}$
10	$\{7, 13, 157, 1051, 9973\}$	$\{3, 7, 991\}$	$\{43_{6^2}, 14783491_{4865581}\}$
11	$\{19, 769, 1451, 19429\}$	$\{2, 3, 7, 97\}$	$\{631_{43}\}$
14	$\{2939, 38377, 47911\}$	$\{2, 3, 19, 2143\}$	$\{13_3, 43_6, 60765967_{27581956}\}$
16	$\{19, 79, 181, 229, 439, 829\}$	$\{2, 3, 7, 2053\}$	$\{43_6, 43933_{9824}\}$
17	$\{7, 13, 31, 743, 3229, 6421\}$	$\{2, 3, 7, 37\}$	$\{157_{12^2}, 937_{322}\}$
19	$\{7, 79, 277, 7219, 130267\}$	$\{2, 3, 7, 1303\}$	$\varnothing$
20	$\{7, 19, 37, 73, 227, 313, 9817\}$	$\{2, 3, 31, 67\}$	$\{1666783_{517555^2}\}$
22	$\{307, 877, 11131, 234193\}$	$\{3, 1466473\}$	$\{7_{42}, 31_{52}, 139627_{11986^2}\}$
25	$\{16249, 390553, 441403\}$	$\{3, 43, 619, 691\}$	$\{19_7, 229_{94^2}, 409_{53}\}$
26	$\{7, 18251, 73417, 456901\}$	$\{3, 367, 10651\}$	$\{13_{3^2}, 91513_{30403}\}$
29	$\{25229, 707197, 785671\}$	$\{3, 57875563\}$	$\varnothing$
31	$\{7, 13, 23, 79, 191, 433, 11689\}$	$\{3, 7, 66523\}$	$\varnothing$
32	$\{67, 15649, 33791, 1153219\}$	$\{2, 3, 3863473\}$	$\{79_{23}\}$
34	$\{7, 40459, 190891, 1461391\}$	$\{2, 3, 3197533\}$	$\{37_{10}, 3181_{440^2}, 236503_{5480^2}, 83666173_{602656^2}\}$
35	$\{11, 19, 61, 211, 26833, 1500523\}$	$\{3, 757, 75931\}$	$\{13_{3^2}, 54499_{23608^2}\}$
37	$\{103, 769, 2437, 19753, 52021\}$	$\{2, 3, 19, 193, 463\}$	$\{73_8, 331_{31}, 811_{130}, 1052203_{452608}, 29322691_{4854914}\}$
40	$\{7, 181, 14143, 65599, 394549\}$	$\{2, 3, 43, 331\}$	$\{19_{7^2}, 674977_{1170352}\}$
44	$\{13, 181, 20707, 87119, 308887\}$	$\{2, 3, 1033, 4129\}$	$\{43_{6^2}, 2341_{1106}\}$
46	$\{11, 127, 349, 9041, 12829, 37657\}$	$\{3, 31, 3563467\}$	$\{67_{29}, 97_{352}, 11503_{467}, 417649_{174641}, 4198807_{268994}\}$
49	$\{13, 19, 31, 127, 2389, 15217, 120049\}$	$\{2, 3, 7, 61609\}$	$\{19801_{21842}\}$
50	$\{59, 67, 241, 2161, 25933, 99109\}$	$\{2, 3, 7, 9130117\}$	$\{331_{31}\}$
52	$\{7, 59, 79, 347, 98101, 7311463\}$	$\{2, 3, 13, 229, 71419\}$	$\varnothing$

n	$\mathcal{D}_{disc}$	$\mathcal{D}_{Cl}$	$\mathcal{F}_{nl}(23\times 10^7)$
55	$\{7, 2749, 3517, 169399, 1307209\}$	$\{2, 3, 7, 14667403\}$	$\{97_{35^2}, 4243_{298^2}, 260047_{18194}\}$
56	$\{13, 43, 277, 823, 2731, 4157, 12613\}$	$\{3, 7, 67, 127, 2719\}$	$\{62434681_{26935694}\}$
59	$\{7, 31, 29837, 390877, 12754741\}$	$\{2, 3, 31, 127, 1327\}$	$\{19_7, 43_6, 19699_{7417^2}, 25357_{9006^2}, 4296091_{2113223}\}$
61	$\{7, 19, 271, 281, 821, 2689, 2078497\}$	$\{3, 613, 388057\}$	$\{37_{10}\}$
62	$\{7, 13, 242171, 1193443, 2110879\}$	$\{3, 31, 3633403\}$	$\{223_{39^2}\}$
64	$\{127, 138493, 266239, 16777027\}$	$\{3, 5011, 129517\}$	$\{43_{6^2}\}$
65	$\{278849, 17850433, 18700243\}$	$\{3, 19, 547, 57697\}$	$\{7_{4^2}, 331_{31}, 3694459_{45444}\}$
67	$\{13, 61, 383, 571, 797, 25411, 36919\}$	$\{3, 7, 1117, 74797\}$	$\varnothing$
70	$\{13, 1933, 12421, 347899, 1928371\}$	$\{2, 3, 4003, 126151\}$	$\{503287_{1125593^2}\}$
71	$\{433, 2683, 9883, 58687, 362951\}$	$\{2, 3, 340422079\}$	$\{7_4\}$
74	$\{59, 6961, 29986357, 31235551\}$	$\{2, 3, 109, 457, 133873\}$	$\{73_{8^2}, 3207019_{467011}\}$
76	$\{7, 23, 61, 317, 823, 5791, 34714219\}$	$\{2, 3, 127, 11237029\}$	$\{19_7, 794641_{291733}, 3728983_{905060^2}, 82044439_{14812302}\}$
77	$\{19, 23, 3583, 9811, 20107, 1924141\}$	$\{3, 1457126959\}$	$\{7_{4^2}, 148942621_{71590090}\}$
79	$\{7, 11, 31, 67, 45389, 581341, 1305391\}$	$\{3, 19, 211, 433, 3631\}$	$\{37_{10^2}, 103_{46^2}\}$
80	$\{7, 13, 19, 31, 67, 103, 719, 20479, 165829\}$	$\{2, 3, 7, 52667059\}$	$\{73_8, 46687_{16066}, 228901_{555292}, 41448541_{53565652}\}$
82	$\{7, 13, 79, 271, 313, 558091, 3477841\}$	$\{3, 13, 1777, 41467\}$	$\varnothing$
85	$\{19, 31, 107, 277, 5807, 6079, 2846677\}$	$\{2, 3, 7, 313, 691, 997\}$	$\{153556531_{38606055}\}$
86	$\{167, 3853, 54700561, 56653879\}$	$\{2, 3, 7, 17713, 51043\}$	$\{73_{8^2}, 6199_{2645}\}$
89	$\{7, 61, 712889, 1028557, 9272173\}$	$\{2, 3, 127, 48593539\}$	$\{31_5, 211_{14^2}\}$
91	$\{631, 829, 919, 2503, 27397, 112339\}$	$\{2, 3, 1483, 52567\}$	$\{73_8\}$
92	$\{17, 19, 373, 2437, 198463, 71639023\}$	$\{2, 3, 61, 193, 542197\}$	$\{103_{46^2}\}$
94	$\{7, 37, 463, 78074617, 90620231\}$	$\{3, 8929, 36396301\}$	$\{67_{29}, 367_{83}, 829_{125}\}$
95	$\{13, 79, 79309, 866399, 84077473\}$	$\{2, 3, 31, 37, 631, 2113\}$	$\varnothing$
97	$\{7, 223, 56713, 922081, 91324339\}$	$\{2, 3, 763707067\}$	$\{19_7, 97_{35^2}, 487_{232}\}$
100	$\{23, 43913, 99999703, 103060603\}$	$\{3, 57709, 1882459\}$	$\{11670859_{4550018}, 54250591_{7365^2}\}$

A.2.2. *Famille de polynômes de Lecacheux.* Voir section 3.2.1.

n	$\mathcal{D}_{disc}$	$\mathcal{D}_{Cl}$	$\mathcal{F}_{nl}(23\times 10^7)$
14	$\{13, 157, 199\}$	$\{3, 13\}$	$\{43_{6^2}, 397849_{1360772}\}$
16	$\{3, 5, 7, 37, 211\}$	$\{3, 43\}$	$\{62347_{4200^2}\}$
22	$\{3, 7, 421, 487\}$	$\{3, 439\}$	$\{151_{32}\}$
26	$\{5, 7, 97, 601\}$	$\{2, 3, 7\}$	$\{523_{60}\}$
28	$\{3, 19, 37, 787\}$	$\{3, 5\}$	$\{331_{312}, 1669_{248}, 640483_{42506}\}$
34	$\{3, 7, 11, 19, 61, 151\}$	$\{3, 7, 19\}$	$\{31_5, 43_{6^2}\}$
38	$\{31, 37, 43, 1447\}$	$\{3, 229\}$	$\{13_{3^2}, 73_8\}$
40	$\{3, 7, 13, 229, 1483\}$	$\{3, 709\}$	$\{73_{8^2}, 28051_{2374^2}, 588277_{199858}\}$
44	$\{7, 13, 43, 139, 277\}$	$\{2, 3, 19\}$	$\{17923_{613}, 8436997_{3980782^2}\}$
46	$\{3, 5, 7, 13, 163, 283\}$	$\{3, 7, 13\}$	$\{31_5\}$
50	$\{7, 13, 181, 2503\}$	$\{2, 3, 37\}$	$\{45439_{2225}, 1602529_{510444^2}\}$
52	$\{3, 17, 2551, 2707\}$	$\{2, 3, 919\}$	$\{7_4, 157_{12^2}, 10453_{270^2}\}$
56	$\{5, 11, 43, 73, 2971\}$	$\{3, 13\}$	$\{7_{4^2}\}$
58	$\{3, 7, 13, 19, 31, 37, 103\}$	$\{3, 17\}$	$\{2221_{543}, 725209_{120249^2}\}$
62	$\{7, 61, 523, 3847\}$	$\{2, 3, 157\}$	$\{13_{3^2}, 14737_{4341}\}$
64	$\{3, 7, 3907, 4099\}$	$\{3, 7, 127\}$	$\{103_{46^2}, 601_{24}\}$
68	$\{7, 67, 661, 4423\}$	$\{3, 13, 31\}$	$\{4621_{1763}, 159622777_{146694922}\}$
74	$\{7, 73, 751, 5479\}$	$\{3, 19, 127\}$	$\{43_6, 107815549_{14774937}\}$
76	$\{3, 5, 7, 13, 61, 5779\}$	$\{3, 1381\}$	$\{400339_{1607152}\}$
80	$\{19, 79, 337, 6163\}$	$\{3, 7, 43\}$	$\{61_{13^2}\}$
88	$\{3, 7, 29, 61, 127, 1069\}$	$\{2, 3, 7, 151\}$	$\varnothing$
92	$\{7, 13, 8191, 8467\}$	$\{3, 1669\}$	$\{367_{83}\}$
94	$\{3, 31, 43, 199, 8839\}$	$\{2, 3, 2851\}$	$\varnothing$
98	$\{13, 67, 97, 139, 739\}$	$\{2, 3, 7, 13\}$	$\{12919_{5520^2}, 247309_{37071}\}$
100	$\{3, 7, 11, 31, 313, 1429\}$	$\{2, 3, 7, 211\}$	$\{13_{3^2}, 6037_{509^2}, 145316557_{177305022}\}$

Références

[1] S. Balady, Families of cyclic cubic fields, *Journal of Number Theory* **167** (2016), 394–406.

[2] S. Balady and L.C. Washington, A family of cyclic quartic fields with explicit fundamental units, 2017, prépublication.

[3] R. Barbelescu and J. Ray, Some remarks and experiments on Greenberg's p-rationality conjecture, 2017, prépublication.

[4] T.W. Cusick, Lower bounds for regulators, Number Theory, Noordwijkerhout, 1983, Vol. 1068, Lecture Notes in Mathematics, *Springer*, *Berlin*, 1984.

[5] C.W. Curtis and I. Reiner, Representation theory of finite groups and associative alegras, Vol. XI, Pure and Applied Mathematics, *Interscience Publishers, John Wiley and Sons*, *New-York London*, 1962.

[6] P. Erdös, Arithmetical properties of polynomials, *Journal of the London Mathematical Society* **28** (1953), 416–425.

[7] J. S. Ellenberg and A. Venkatesh, Reflection principles and bounds for class group torsion, *Int. Math. Res. Not. IMRN* **1** (2007), Art. ID rnm002, 18.

[8] G. Gras, Heuristics in direction of a p-adic Brauer–Siegel theorem, 2018, prépublication.

[9] G. Gras, A program to test the p-rationality of any number field, 2017, prépublication.

[10] G. Gras, The p-adic Kummer-Leopoldt Constant - Normalized p-adic Regulator, *International Journal of Number Theory* **14 No. 2** (2018), 329–337.

[11] G. Gras, Les Θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques, *Canadian Journal of Mathematics* **68** (2016), 571–624.

[12] G. Gras, Class Field Theory, From Theory to practice, *Springer-Verlag*, *Berlin*, second corrected printing 2005.

[13] G. Gras and J.-F. Jaulent, Sur les corps de nombres réguliers, *Mathematische Zeitschrift* **202** (1989), 343–365.

[14] R. Greenberg, Galois representations with open image, *Annales Mathématiques du Québec* **40, 1** (2016), 83–119.

[15] J.-F. Jaulent and T. Nguyen Quang Do, Corps p-réguliers, corps p-rationnels et ramification restreinte, *Journal de Théorie des Nombres de Bordeaux* **5** (1993), 343–363.

[16] H. Koch, Galoissche Theorie der p-Erweiterungen, *Deutscher Verl. der Wiss.*, *Berlin*, 1970.

[17] Y. Kishi, A family of cyclic cubic polynomials whose roots are systems of fundamental units, *Journal of Number Theory* **102** (2003), 90–106.

[18] S. Lang, Algebraic Number Theory, Graduate Texts in Mathematics, *Springer-Verlag*, *New York/Berlin*, 1986.

[19] O. Lecacheux, Units in number fields and elliptic curves, In Advances in number theory (Kingston, ON, 1991), Oxford Sci. Publ., *Oxford Univ. Press*, *New York*, 1993, 293–301.

[20] C. Maire, Sur la structure Galoisienne de certaines pro-p-extensions de corps de nombres, *Mathematische Zeitschrift* **267** (2011), 887–913.

[21] C. Maire, Une estimation de la dimension de Krull des anneaux de déformations en ramification incomplète, *Publications Mathématiques de Besançon* (2006), 13pp.

[22] E. Maus, Computation of Integral Bases in Certain S_n Extensions of $\mathbb{Q}$, *J. Symbolic Computation* **4** (1987), 99–102.

[23] A. Movahhedi and T. Nguyen Quang Do, Sur lâĂŹarithmétique des corps de nombres p-rationnels, Séminaire de Théorie des Nombres, Paris 1987–88, Vol. 81, Progr. Math., *Birkhäuser Boston*, *Boston, MA*, 1990, 155–200.

[24] T. Nguyen Quang Do, Formations de classes et modules dâĂŹIwasawa, Number theory, Noordwijkerhout 1983, Vol. 1068, Lecture Notes in Mathematics, *Springer*, *Berlin*, 1984, 167–185.

[25] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, Vol. 323, GMW, *Springer-Verlag*, *Berlin*, 2000.

[26] The PARI Group, PARI/GP version `2.9.4`, *Univ. Bordeaux*, 2018, http ://pari.math.u-bordeaux.fr/.

[27] F. Pitoun and F. Varescon, Computing the torsion of the p-ramified module of a number field, *Mathematics of Computation* **84 291** (2015), 371–383.

[28] M. Rougnant, Sur quelques aspects des extensions à ramification restreinte, Thèse, Université Bourgogne-France-Comté, 2018.

[29] J.-P. Serre, Cohomologie Galoisienne, Vol. 5, Lecture Notes in Mathematics, *Springer–Verlag*, *Berlin*, 1994.

[30] A. Schmidt, On the relation between 2 and ∞ in Galois cohomology of number fields, *Compositio Math.* **133 3** (2002), 267–288.

[31] L.C. Washington, Introduction to Cyclotomic Fields (2nde ed.), Vol. 83, GTM, *Springer-Verlag*, *New-York*, 1997.

[32] K. Wingberg, Free quotients of Demushkin groups with operators, 2004, prépublication.

[33] K. Wingberg, Galois groups of local and global type, *Journal Reine Angew. Math.* **517** (1999), 223–239.

[34] K. Wingberg, On Demushkin groups with involution, *Annales Scientifiques de l'É.N.S. 4ème série* **22 4** (1989), 555–567.

UNIVERSITE BOURGOGNE FRANCHE-COMTE
FEMTO INSTITUTE, CNRS
15B AVENUE DES MONTBOUCONS
25030 BESANCON CEDEX, FRANCE

LABORATOIRE DE MATHEMATIQUES DE BESANCON
UMR CNRS 6623
UFR SCIENCES ET TECHNIQUES
16 ROUTE DE GRAY
25030 BESANCON CEDEX, FRANCE

E-mail: christian.maire@univ-fcomte.fr

UNIVERSITE BOURGOGNE FRANCHE-COMTE
LABORATOIRE DE MATHEMATIQUES DE BESANCON
UMR CNRS 6623
UFR SCIENCES ET TECHNIQUES
16 ROUTE DE GRAY
25030 BESANCON CEDEX
FRANCE

E-mail: marine.rougnant@univ-fcomte.fr